Human-Centric Intelligent Systems (2023) 3:312–343
https://doi.org/10.1007/s44230-023-00025-3

REVIEW ARTICLE

A Comprehensive Survey on Machine Learning using in Software Defined Networks (SDN)

Sahar Faezi[1] · Alireza Shirmarz[1]

Received: 6 March 2023 / Accepted: 15 May 2023 / Published online: 8 June 2023

Abstract

These days, Internet coverage and technologies are growing rapidly, hence, it makes the network more complex and heterogeneous. Software defined network (SDN) revolutionized the network architecture and simplified the network by separating the control and data plane. On the other hand, machine learning (ML) and its derivations have made the systems more intelligent. Many pieces of research papers have addressed ML and SDN. In this survey, we collected the papers published in Springer, Elsevier, IEEE, and ACM and addressed SDN and ML between 2016 and 2023. The research papers are organized based on the solutions, evaluation parameters, and evaluation environments to help those working on SDN and ML for improving the target functional or non-functional parameters. The research papers will be analyzed to extract the solutions, evaluation parameters and environments. The extracted solutions, evaluation parameters and environments will be clustered in this review paper. The research gap and future research directions will be stated in this work. This survey is completely useful for those who working on SDN and want to improve the functional and non-functional parameters using machine learning.

Keywords Software defined networks (SDN) · Machine learning (ML) · Deep learning (DL) · Security · Routing · Performance

Abbreviations

SDN	Software defined networks
ML	Machine learning
DL	Deep learning
AI	Artificial intelligence
QOS	Quality of service
SL	Supervised learning
UL	Unsupervised learning
RL	Reinforcement learning
MBF	Multiple bloom filters
LR-DDoS	Low-rate distributed denial of service
IP	Internet protocol
EFDT	Extremely fast decision tree
DT	Decision tree
DT-SVM	Decision tree_support vector machine
SVM	Support vector machine
DNS	Domain name system
SSIM	Structural similarity index measure
SDNFV	Software-defined network function virtualization
AMLSDM	Adaptive machine learning services attacks detection and mitigation
MLMR	Machine learning based multipath routing
SRDO	Smart ranking-based data offloading
GRU	Gated recursive unit
RNN	Recurrent neural network
LSTM	Long-short-term memory
DRL-SMS	Deep reinforcement learning_SMS
MDP	Markov decision process
DLCPP	Deep learning-based content popularity prediction
CNN	Convolutional neural network
ONOS	Open network operating system
IED	Intelligent electronic devices
DMLCA	Deep machine learning in cyber space called cantina
CCO	Control channel overhead
CUC	CPU usage of the controller
GRU	Gated regression units
MOO	Multi-objective optimization
GAN	Generative adversarial network

✉ Alireza Shirmarz
a.shirmarz@aut.ac.ir

Sahar Faezi
saharfaeziii@gmail.com

[1] Department of Computer and Electronic Engineering, Ale-Taha Institute of Higher Education, Tehran, Iran

IDS	Intrusion detection systems
CIDS	Common intrusion detection system
IID	Independent identity distribution
ARIMA	Automatic regression integrated moving average

1 Introduction

These days, Internet coverage and quality are growing rapidly; hence, the diversity and complexity of the network have caused the network architecture to be forced to change. Today's network needs to be programmable, agile and flexible, such as a software defined network (SDN) which is an architecture [1]. The SDN architecture has made the network more programmable and flexible by separating the data plane from the control plane. This architecture simplifies the network with a centralized controller. This architecture has three layers, including data, control and application layers. In addition, it has three APIs consisting of northbound, southbound and east–west APIs. The SDN architecture is shown in Fig. 1. Northbound API is used to connect the application layer and control layer. Southbound API is for connecting the data layer to the control layer. East–west API has been proposed to scale up the control layer and improve the scalability of SDN because it causes the controllers to be connected and make distributed controllers which are named the conceptual centralized controller against the physical centralized controller [1]. On the other hand, machine learning (ML) has given the ability of decision to the system which has made the computing system more intelligent. This capability can be used in SDN with various applications, especially in the control layer as the decision maker in SDN architecture [1]. ML has been used to improve network performance, security, Quality of Service (QoS), and other non-functional concepts in SDN. ML can be categorized into four general groups: (1) supervised learning, (2) unsupervised learning, (3) semi-supervised learning, and (4) reinforcement learning [2][2].

In the wide range of research papers related to SDN, ML has been proposed to be used in SDN for different applications and improvement targets, so we review the recent research papers to extract the improvement targets and the solutions which have been proposed. The contributions of this paper are:

- Review the recent research papers between 2016 and 2023 which are related to SDN and machine learning. Well-known journals, including Elsevier, Springer, IEEE, and ACM are the resource target of this paper.

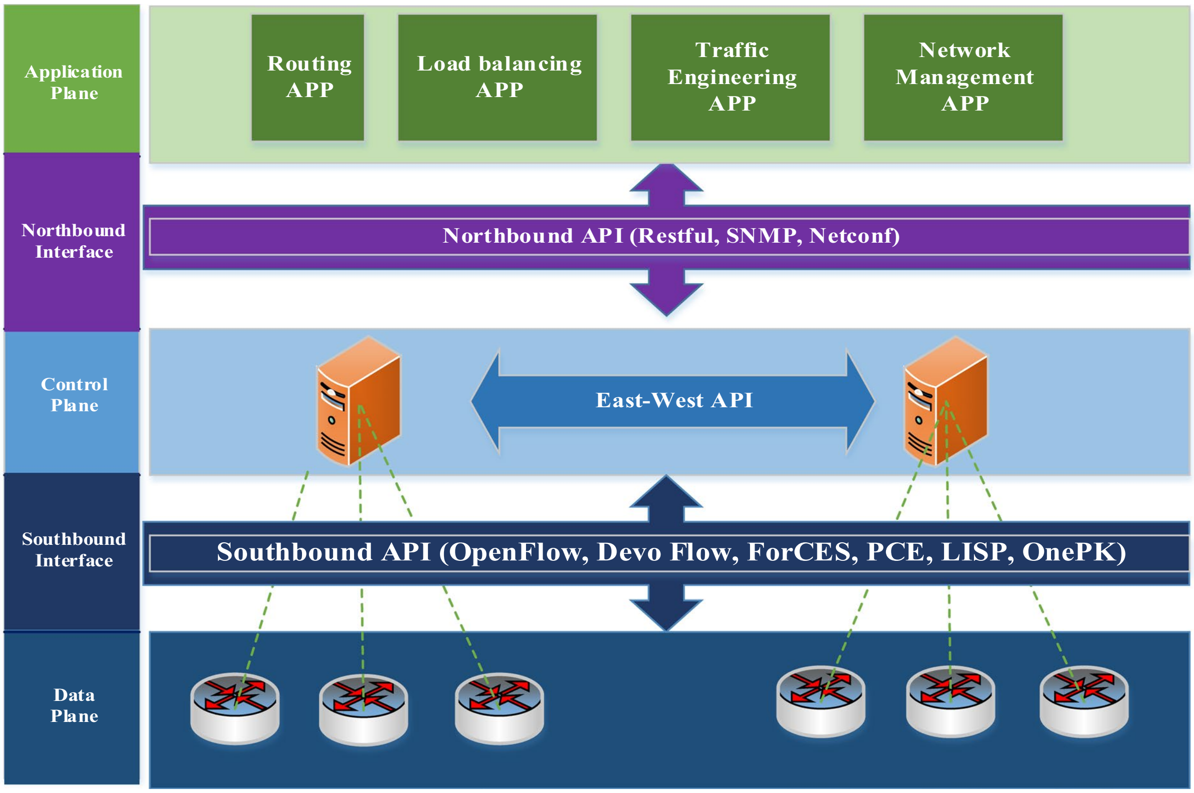

Fig. 1 Architectural planes of SDN [1]

- The Software Defined Network (SDN) and Machine learning are the two key words which different form of these words and other derivations of these key words are used for this survey in the mentioned resources.
- The proposed approaches in recent research papers for SDN which are based on a wide range of machine learning techniques are extracted and categorized in this survey.
- The functional and non-functional improvement targets and the effective metrics are extracted in this survey according to the recent research papers published.
- The gap research topics can be used in future work for improvement in SDN using machine learning.

This survey is useful for those working on SDN to improve the non-functional parameters while using ML because this survey indicates the research gap and future direction related to SDN and ML.

The process of this survey has the steps: search, paper recognition, review, research refinement, selected papers and preparing the articles which are shown in Fig. 2.

In this paper, the published papers between 2016 and 2023 are reviewed and ML techniques used in SDN architecture are extracted. The improvement targets that the research papers have placed at the center of attention, such as network performance, efficiency, intelligence and security are discussed in this paper. The proposed solutions are examined and categorized from different aspects in this paper. Finally, we will discuss the challenges of ML usage in SDN and the direction of proposed solutions. In the following, Sect. 2 will address the review papers regarding ML in SDN. Section 3 will state the research papers and elaborate on their problem and solutions. Section 4 will express the ML usage in SDN and illustrate the future direction and, the conclusion will be stated finally.

2 Related works

The review papers which have addressed SDN and ML are considered for the related work. Five review papers related to SDN and ML have been found in this research. Xie et al. reviewed machine learning algorithms used in SDN in terms of quality of service (QOS)/quality of experience (QoE) prediction, routing optimization and traffic classification using machine learning algorithms. The research papers published in 1989–2017 have been investigated in [2]. Shirmarz et al. have investigated the issues and solutions proposed in the research papers for network performance improvement in SDN between 2011 and 2019. They classified the research papers based on their applications: wide area network (WAN), wireless network, and cloud computing/fog computing. They have searched IEEE, Springer, Elsevier, and ACM to find the research papers. One of the solutions extracted in their work is ML which is used for performance improvement in various applications [1]. R. Amin et al. have discussed one of the ways to optimize routing in SDN, so they addressed ML techniques divided into three categories supervised, unsupervised and reinforcement learning. The research papers published between 2005 and 2021 are considered in their survey [3]. Ebneyousef et al. have surveyed to extract fog load balancing algorithms, system architecture, tools and applications, and their advantages and disadvantages among the articles published between 2018 and 2022 in Springer, Elsevier, IEEE, and ACM [4]. Mohammadi et al. focused on network traffic engineering in SDN between 2017 and 2022. The network traffic engineering in SDN has been done with different solutions and one of the most significant research of them is ML [5]. Jiang et al. have worked on graph-based deep learning for communication networks and surveyed the approaches proposed for different types of communication networks e.g. wireless, wired, and software defined networks. They addressed the problems solved with graph-based deep learning [6]. The abstract of the reviewed articles is given in Table 1.

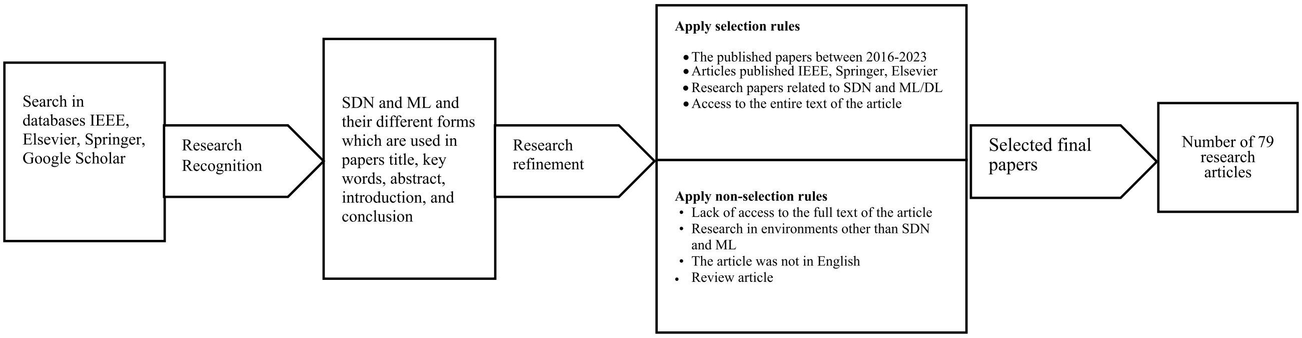
Search in databases IEEE, Elsevier, Springer, Google Scholar
Research Recognition
SDN and ML and their different forms which are used in papers title, key words, abstract, introduction, and conclusion
Research refinement
Apply selection rules
• The published papers between 2016-2023
• Articles published IEEE, Springer, Elsevier
• Research papers related to SDN and ML/DL
• Access to the entire text of the article
Apply non-selection rules
• Lack of access to the full text of the article
• Research in environments other than SDN and ML
• The article was not in English
• Review article
Selected final papers
Number of 79 research articles

Fig. 2 Criteria for selection of research papers

Table1. List of review articles

References No	Years which addressed	Published Year	Publisher	Main Background
[1]	2011–2019	2020	Springer	Performance issues and solutions in SDN-based data center: a survey
[2]	1989–2017	2018	IEEE	A survey of machine learning techniques applied to software defined networking (SDN): research issues and challenges
[3]	2005–2021	2021	IEEE	A survey on machine learning techniques for routing optimization in SDN
[4]	2018–2022	2023	Springer	A taxonomy of load balancing algorithms and approaches in fog computing: a survey
[5]	2017–2022	2022	Springer	Taxonomy of Traffic Engineering Mechanisms in Software-Defined Networks: A survey
[6]	2017–2021	2022	Elsevier	Graph-based deep learning for communication networks: A survey

All the review papers which are close to ML and SDN are limited and they have addressed the network non-functionalities improvement they found machine learning a significant approach which is at the center of researchers' attention. This review paper addresses the ML and SDN to narrow the research topic; therefore, the research papers which are related to these two key words are examined to extract the solutions, metrics and target improvements (functional and non-functional) concept in SDN architecture. In this review paper, the SDN and ML are the key words, which different forms and derivations of them are searched in the Springer, Elsevier, IEEE, and ACM, but the other found papers are considered as well to enrich this review paper. Furthermore, the research papers had been published in the years between 2016 and 2023 are examined and the distribution od published papers is shown in Fig. 3.

In the following section, the research papers are elaborate and categorized in various aspects.

3 Machine Learning Usages in Software Defined Networking

In recent years, with the advancement of technology and the rapid growth of the Internet and mobile communication technologies, the infrastructure, devices and resources in network systems have become more advanced and complex. To manage and organize and optimize and maintain network systems, a lot of information must be considered and used. However, it was difficult to use machine learning in traditionally closed networks, SDN revolutionized the network flexibility, agility and programmability and make the opportunities for the researchers to work on different aspects of the network using software-based solutions. ML is a significant approach which can be used in SDN architecture to improve network functionalities and non-functional parameters such as performance, security, and others. Ml is a concept, that includes three main components: Model,

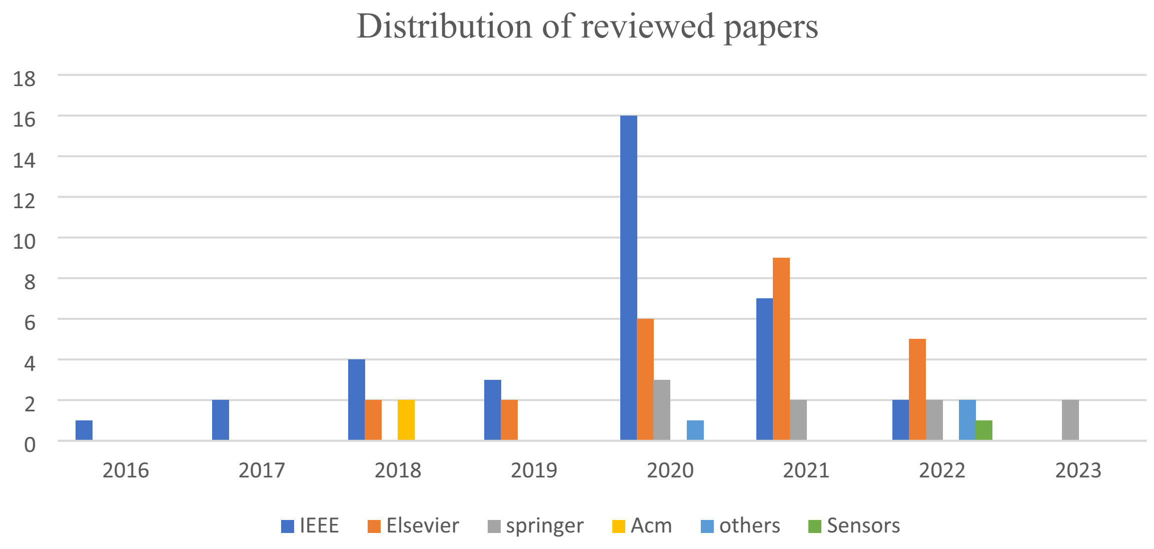

Fig. 3 Distribution of papers

Parameters, and Learning system. The model predicts or identifies, the parameters are the signals or factors used by the model to improve the prediction/classification performance. The learning system is a system which is used to train, evaluate and test the model with training and test sets.

In [3], all the ML techniques have been examined which include three categories: reinforcement learning, unsupervised learning, and supervised learning and are used to optimize routing in SDN. The existing one has been specified.

In [7], in this article, the controller is programmed in such a way that it has an internal mechanism so that the traffic flows suspended in the buffer cannot be deleted and it no longer waits for the response of the application page.

In [8], the authors have worked on a proposed plan to improve security in today's networks. Based on SDN, a multi-target flow routing scheme is enabled for effective data delivery. They have compared the proposed model with other advanced models and have checked Weber on data sets such as CMU, KDD'99, and TIET, and the results show the better performance of this model.

In [9], the researchers have investigated the systematic performance using a software-based network simulator. They have simulated the network elements and conducted experiments based on deep RL and traditional RL algorithms. The results show a reduction of about 60 It has shown a percent long-term control overhead and about 14% increase in table hits concerning flow table with a fixed size of 4 KB compared to the Multiple Bloom Filters (MBF) method. They believe that their work is the first to use RL to manage flow inputs in SDN and this has not been done before.

In [10], the authors have worked on identifying ransomware. They have proposed a method where ransomware can be detected by signatures of network traffic. They have combined the high processing rate of new hardware-based stream generators with the high-performance and parallel RaftLib framework for ransomware classification and stream feature extraction.

In [11], the authors have investigated LR-DDoS attacks and proposes a flexible modular architecture to mitigate LR-DDoS attacks. This architecture has made it possible to detect and mitigate attacks in SDN settings.

In [3], the authors have worked to optimize routing in SDN using ML techniques based on reinforcement learning, unsupervised learning, and supervised learning.

In [12], the authors have examined complex network security and described methods of using machine learning with SDN to enable complex network security. These operations include honeypot rerouting, botnet detection, and anomaly detection. They are learning operations. SDN machines and control have been used for the distribution, scaling, and architecture of complex network systems and their existing solutions. Using a Mininet-based testbed, they have also investigated the supervised learning aspect of the overall system.

In [13], the authors have worked on the classification and detection of conflicting flows in SDN and have presented several machine learning algorithms. They have classified existing conflicts based on IP source address, action, protocol, and priority of flow rules. Four algorithms have been used, which are very fast decision tree (EFDT), decision tree (DT), hybrid (DT-SVM), and support vector machine (SVM). Among them, EFDT and DT-SVM dual-algorithms were developed based on DT and SVM algorithms, respectively, to increase their performance in terms of efficiency and effectiveness. In this article, in addition to the aforementioned works, they have designed two network topologies, which are called Fat Tree Topology and Simple Tree Topology.

In [14], the researchers have proposed and evaluated ML techniques to deal with DoS and DDoS attacks in SDN. These techniques are evaluated practically in a practical setting. They investigated the results by exposing the SDN controller to DDoS attacks to make important decisions for security based on ML techniques for future communication networks.

In [15], a scheme has been proposed to prevent Domain Name System (DNS) amplification attacks in the context of SDN software-defined networks (the largest Distributed Denial of Service (DDoS) attack) to protect the permission blockchain nodes. The name of the proposed scheme is BrainChain which is a scalable and efficient plan.

In [16], a model called Deep-SDN has been proposed, which is a new deep-learning model for software-defined networks. This model can accurately identify a wide range of traffic applications in a short period. The performance of the proposed model has been compared with the latest technology in this field. The results of the investigations show that the proposed model has better results in terms of accuracy, recall, and F-score. With the proposed model, an overall accuracy of 96% can be achieved.

In [17], a technique called decision tree (DT) and support vector machine (SVM) have been used to identify malicious traffic, and it is one of the machine learning techniques. They have conducted experiments and the results show that the proposed technique has better accuracy and detection rate.

In [18], the authors have worked on predicting the quality of experience (QoE) in SDN networks based on complete reference parameters (SSIM, VQM) and application metrics (resolution, bit rate, frame rate).

In [19], a new container-based architecture with different fog nodes has been proposed to solve the problem of resource allocation in geographically distributed heterogeneous fog networks. By using this architecture, it is possible to have deep learning Q-network-based resource allocation for

Solving the resource allocation problem that has different components.

In [20], an intelligent defense system has been proposed to implement the machine learning agent, which can process the current state of the network. This defense system takes a set of necessary actions in the form of network flows defined by The software.

In [21], machine learning algorithms trained on historical network attack data have been used to identify potential malicious connections and potential attack targets.

In [22], a combination of statistical techniques and machine learning has been used to detect high-volume and low-volume DDoS attacks.

In [23], a software-defined network function virtualization (SDNFV) network for network augmentation has been suggested for security and network scalability improvement. In this research, stateful firewall services are placed as VNFs in the SDN network. A set of guidelines and rules are established by the SDN controller to prevent dangerous network connectivity.

In [24], the authors have worked on the mitigation of attacks and proposed an attack detection and mitigation (AMLSDM) framework based on adaptive machine learning. To successfully identify and mitigate DDoS attacks with the support of an adaptive machine learning classification model, the AMLSDM framework, which is a security mechanism that provides SDN capability for IoT devices.

In [25], the authors suggested an approach to identify and protect the open flow (OF) switch controller against DDoS attacks. An SDN framework is designed. Their proposed framework is to train a machine learning model based on the data taken to predict DDoS attacks.

In [26], the security of the SDN environment against DDOS attacks has been investigated, discussed and analyzed the schemes based on machine learning. They have examined the criteria such as strengths and weaknesses, performance, and datasets. To evaluate the performance of a set of classification algorithms that are widely used to detect DDoS attacks, all of which are based on machine learning in an SDN environment, they used the 2019 CIC-DDoS dataset and challenges and have explored the future paths for the development of these projects.

In [27], a machine learning-based multipath routing (MLMR) framework considering the flow rule space constraints and quality of service (QoS) constraints have been proposed for software networks.

In [28], a new reputation-based blockchain called PoolCoin based on a distributed trust model for mining pools has been suggested. This trust model used by this blockchain is inspired by the labour market signalling model.

In [29], the authors examined, categorized, and compared various advanced plans for detecting and reducing anomalies in SDN. This article, by reviewing studies, showed that the most important external threats in SDNs are DoS attacks. that the collection of statistical data has been done by various methods and the anomaly detection algorithm should be considered for it because the comparison and analysis of the reports show that the data collection is generally done using the native OpenFlow protocol in networks with traffic has been high, which leads to the saturation of the control level. As a result, special protocols are needed to collect data.

In [30], the SDIoT networks have been scrutinized and presented a new solution called Deep Place has to establish the flow rule to provide a detailed traffic analysis capability adaptively. Also, by doing this, flow table overflow can be avoided. and ensure the QoS implementation of the traffic flow. At the same time, they have formulated the optimization problem based on the MDP framework to deal with the traffic dynamics of the Internet of Things and to achieve the control policy, they have developed an algorithm based on the gradient of the deep deterministic policy.

In [31], an entropy-based active learning model has been combined with the effective detection of intrusion patterns at the packet level. This model, which is developed as a load balancer, can track the attack in the network. Also, a load-balancing algorithm Able to optimize sensor computations and resource requirements in automotive sensors has been presented.

In [32], the authors combined multi-class semi-supervised machine learning in SDN and deep packet detection and proposes an architecture based on it. Based on the proposed architecture, the network can achieve fine adaptive QoS traffic engineering because the proposed architecture can classify into different QoS categories. The network can also maintain a dynamic flow database through deep packet detection techniques.

In [33], a smart ranking-based data removal (SRDO) algorithm has been proposed to select an RSU and improve service quality. SRDO is used to select RSU in the Q-Learning algorithm. Also, to solve the problem of RSU selection in an intelligent way to dump data, this algorithm is modelled in the software-defined network controller.

In [34], deep learning algorithms are used to protect the controller by applying high-security measures, which are essential for continuous connectivity in the network and availability. In addition to this Gated Recursive Unit (GRU), recurrent neural network (RNN) and long-short-term memory (LSTM) have been proposed to prevent intrusion attacks and identify them. All the models in this paper have been evaluated using the In SDN dataset.

In [35], a switch migration strategy based on deep reinforcement learning (DRL-SMS) has been suggested to solve the problem of load imbalance in the multi-controller control plane. In this strategy, the set of migration actions and system reward, modelling analysis for SDN for obtaining the state of the system is done based on the Markov decision process (MDP). Using double deep Q-Network (DDQN), the approximate function fitting is obtained with the Q values of the switch migration actions and then optimized by the Q-parameters. DDQN training network is given using the experience replay mechanism. Also, after training, it calculates DRL in the current state of the system using a strategy based on Q-value, then selects the maximum Q-value to perform switch migration. Experiments in the environment Simulations show that the proposed strategy greatly reduces the balancing time and has a great effect on balancing the controller load.

In [36], machine learning (ML) has been utilized based UAV management framework in Software Defined Networks (SDN). In the proposed framework, the authentication and communication rules are compared to their application by the SDN controller of ML according to the radio frequency feature. The drone is specified and determined.

In [37], an unsupervised hybrid machine learning approach has been used for intrusion detection in SDNs based on automatic encryption. The experimental results show that the proposed module achieves high accuracy with the minimum number of currents selected. Also, the investigations on the performance of the controller with the established model show that for the throughput and delay that were tested, regarding the performance of the SDN controller, even though there is minimal overhead, it has very high detection accuracy at the same time.

In [38], Deep Learning Based Content Popularity Prediction (DLCPP) to obtain the popularity prediction has been used in this research. The proposed model to create a distributed deep learning network that can be reconfigured from the computing resources of switches and links in it uses SDN.

In [39], a routing module has been designed for software-defined networks that are based on machine learning. The proposed module will be able to classify traffic matrices to provide real-time routing decisions by learning optimal routing solutions from historical traffic traces.

In [40], a machine learning framework called MER-SDN has been offered for the topic of traffic-aware energy-efficient routing in SDN. The three main stages of machine learning are feature extraction, training, and testing. All experiments have been performed using real-world network topology and dynamic traffic tracing from SNDlib on Mininet and POX controller. The results of the tests show that in the proposed approach, a 65% reduction in the feature size, and 70% accuracy has been achieved in the parameter prediction of an energy-efficient exploratory algorithm.

In [41], an architecture is proposed for the timely detection of threats and multi-vector attacks, which is based on hybrid DL and has Cuda capability. The proposed architecture uses a convolutional neural network (CNN) and predictive power of short-term memory (LSTM) threats and Detect multi-vector attacks.

In [42], an architectural model has been suggested to solve the problem of load balancing in SDN networks. The proposed model combines machine learning algorithms with segment routing to achieve better performance and network load balancing. The proposed architecture model facilitates the ability to predict the overload of network paths by improving QoS, and this is one of the main advantages of this model.

In [43], a hybrid machine was proposed to protect the controller against DDoS attacks. This hybrid machine is a learning model. Examining the results shows that the detection rate, warning rate, and accuracy in the hybrid machine model are less wrong compared to the simple machine learning models.

In [44], the authors have studied the automatic classification of network data based on machine learning. In the study, several machine learning algorithms from the ONOS (Open Network Operating System) platform were used to automatically classify collected real network traffic data. Experiments have been conducted with simple network topology; the results show that machine learning algorithms can effectively classify network traffic data. Also, the results show that if they use machine algorithms blindly, they will show limited performance.

In [45], the authors have reviewed and analyzed the studies that have used unsupervised and supervised learning techniques. The methods of learning or semi-supervised learning that have been used to solve problems in SDN have been analyzed and categorized.

In [46], the authors investigated and evaluated the security risks in a communication network of a smart network equipped with SDN and presents a framework. It specifically investigates DoS attacks on intelligent electronic devices (IED) and the IEC 61850 network and quantifies its risks. The proposed model is a security score model that considers the critical role of each IED device and evaluates its impact on the overall network of the smart grid. By examining the model, they show how SDN frees the smart grid network from congestion and improves the scheduling performance of IEC 61850-type messages, and makes their time compatible.

In [47], the authors have discussed a new framework based on a software-defined network with the help of deep machine learning in cyberspace called CANTINA (DMLCA) for the prevention of phishing attacks. The proposed approach is based on SVM (Support Vector Machine) to deal with the phishing attack problem. This approach is based on machine learning.

In [48], a highly scalable and efficient combination of DL SDN framework called IoMT for malware detection has been suggested. The proposed mechanism does not impose any additional constraints on IoT resource-limiting factors. The results show that the proposed mechanism performs better to identify IoMT for subsequent reduction and prevention. Also, this mechanism does not require much computational complexity.

In [49], a monitoring approach for software-defined networks called IPro has been proposed. This approach is an architecture based on the knowledge-defined network paradigm and an IPro prototype, which is a reinforcement learning-based algorithm. This approach uses Reinforcement Learning to determine the exploration distance, which keeps the control channel overhead (CCO) and additional CPU usage of the controller (CUC) at a threshold.

In [50], the incremental strategy consideration in SDN, which is called hybrid strategy, has been proposed which is a technique called PrePass-Flow. It is based on machine learning to reduce the impact of network layer failure in hybrid SDN. This technique can predict link failures before they occur and proactively install ACL policies at calculated locations after recalculating their location.

In [51], the ways to achieve a guaranteed QoS for data flows have been examined and proposes an intelligent routing mechanism with a QoS guarantee called QI-RM in SDN. The proposed mechanism has been tested in the simulation environment and the results show that MACCA2-RF&RF can classify the data streams efficiently with 99.73% identification accuracy and QI-RM can guarantee the QoS requirements of the data stream before and after link congestion.

In [52], a recognition system based on machine learning has been introduced to improve the security of SDN-based Internet of Things architecture. This approach detects anomalies using the limited Boltzmann machine. By examining the evaluations and the results of the tests in the simulated environment, it shows that the accuracy rate is more than 94%, which is very significant.

In [53], the DRL-R deep reinforcement learning-based routing has been proposed, which is a routing scheme with resource recombination mode, for the routing issue in SDN. The effectiveness of the proposed design has been investigated in a wide simulation environment. The results show that DRL-R has higher throughput, lower flow completion time, better robustness, and better load balance compared to OSPF.

In [54], To prevent attacks in SDN, the researchers, in this article, introduce a defense system that is based on IP flow sources obtained from IP flow analysis and uses the deep learning method of gated regression units (GRU) to identify DDoS attacks and intrusions. This approach is a type of direct flow inspection that enables faster mitigation responses and greatly reduces and minimizes the impact of attacks on SDN.

In [55], the authors, by studying flow control issues, have proposed a priority-based model using SDN. In this model, the function is that the data packets through the network ensure the implementation of the bandwidth and the virtual circuits perform the reallocation work. The machine learning model monitors all system network behaviours in abnormal and normal traffic data transmission to identify abnormal intruders.

In [56], a new service migration scheme to support mobility has been suggested. In this article, in the MEC environment, the problem of multi-user service migration is studied, and based on the investigations, a scheme called DRLMSM is proposed based on DRL technology to optimize the average total cost.

In [57], a new approach called IoT-Train-Deep for smart software-defined networks has been introduced. In this article, they have tried to embed network intelligence in the flow transmission architecture of software-defined networks through a deep Boltzmann machine and incremental tensor train decomposition model. The results of the evaluations based on the amount of delay, throughput, and storage space according to the variation in the number of traffic flows, request rate, table occupancy index, and the number of flow entries show that the proposed model has made significant improvements.

In [58], the routing in SDN using machine learning (ML) based techniques has been used and an approach that is based on ML and multi-objective optimization (MOO) techniques has been proposed. Also for this approach using an ML-based algorithm, the reliability of links is evaluated in a software-enabled multi-hop (SDN) scenario for an IoT-fog environment. The evaluation results show that the Pareto-optimal set of App-1 communication through the chosen path completed its execution in 13% less time than communicating through the shortest path. App-2 had 41% less packet loss using the selected path compared to using the shortest path.

In [59], a hybrid complex neural network-short-term memory (CNN-LSTM) model was introduced to detect DDoS attacks in SDN-based networks. Performance evaluations of this model based on customized data sets had very good and impressive results Performance criteria were above 99%.

In [60], an adversarial testing tool for the robustness of supervised and unsupervised machine learning classifiers against adversarial attacks has been suggested. This test tool can create hostile attacks and disrupt various traffic characteristics. Now, considering a test platform that this article used the same supervised and unsupervised machine learning classifiers, this tool is tested. The results show that the detection performance of the proposed detection system decreases with the creation of hostile attacks.

In [61], a detection and defense system has been proposed that uses the Generative Adversarial Network (GAN) framework and is based on Adversarial training in SDN to detect

DDoS attacks and applies adversarial training to make the system less sensitive to adversary attacks. This system uses IP flow analysis to continuously monitor the traffic using well-defined modules and enables the anomaly detection system to operate in near time.

In [62], the authors examine the security of drone communications and preventing attacks on drone networks with the help of machine learning and software-defined networks. By examining the previous studies on the identification of two main types of attacks in the drone network, i.e.: penetration from the outside and use of the network from the inside, it has addressed the attacks from the outside and examined the strength of the Software Defined Network (SDN) architecture in facing it. Based on SDN flow counters, a traffic injection detection technique and corresponding countermeasures have been proposed. In addition, a new machine learning solution based on random forest classification has been presented to deal with insider attacks that only rely on stream creation events.

In [63], a modular and flexible SDN-based architecture that uses multiple machine learning (ML) and deep learning (DL) models has been proposed to detect transport and application layer DDoS attacks. By examining various ML/DL methods, they have investigated the methods so that they can find a more suitable method for detecting attacks. In this article, ML/DL models have been tested using two security data sets, which are: CICDoS2017 and CICDDoS2019 data sets and the results have shown 99% accuracy in invisible traffic classification. In addition, using the Mininet network simulator and SDN controller of the open network operating system (ONOS), they have implemented a simulation environment, which evaluation results show a detection rate of over 98% for transport DDoS attacks and up to 95% for DDoS attacks have been the application layer.

In [64], the security threats and intrusion detection systems (IDS) have been investigated and designed a common intrusion detection system (CIDS) for VANETs using deep learning with generative adversarial networks. Subscribers can only train a global intrusion detection model for the entire network without directly exchanging the intrusion detection model. With the evaluations, it was determined that the mentioned sub-network streams proved their CIDS accuracy in both IID (independent identity distribution) and non-ID conditions. This work was done through experimental evaluation and theoretical performance analysis on the real-world data set detailed experimental results showed that the proposed CIDS is efficient and effective in intrusion detection for VANET.

In [65], a framework called HuMOR has been proposed, which is a software-defined network (SDN) modular transport management framework, to create and evaluate and verify QoS-preserving transmission algorithms. In addition, they have introduced ABRAHAM based on the capabilities of HuMOR, which is a machine learning-supported proactive and proactive forwarding algorithm that uses many metrics to predict future network conditions and improve AP load to ensure QoS is maintained. Also, ABRAHAM has been compared with alternative handover algorithms in IEEE 802.11, SDN, and handover algorithm, and the evaluation results showed that it has improved performance by 139%.

In [66], the two forecasting models for SDN controller load forecasting based on automatic regression integrated moving averages (ARIMA) and long-term short-term memory (LSTM) approaches have been used for this research. The two forecasting models have been compared in terms of accuracy and error in forecasting. Is. The evaluation results show that in long-term forecasts, the accuracy of the LSTM model is 55% better than ARIMA in terms of forecast errors. In addition, to select the components of the data plane for migration and where the migration should occur under delay constraints, formulating the problem as a non-linear binary program is proved to be NP-complete and a reinforcement learning algorithm is proposed for this. The proposed algorithm was simulated and the results showed that the proposed algorithm has a better performance than the recent benchmark algorithms from the literature and has worked close to optimal.

In [67], an approach for intelligent detection of DDoS attacks in SDN networks called Kulbak-Leibler has been proposed. The proposed approach to detect flow anomalies during the session works by comparing the average session time with the access time to the server from specific IP addresses and the obtained values are recorded in the machine learning database. The increase in the duration of access to the service, which has been seven days here, is re-compared and the value of KL is again determined and written in the ML database. By analyzing service length and access prescription rules, the controller detects anomalies in flow admission requests with KL accumulation values in an ML. As a result, the SDN controller detects the IP domains that DDoS attacks from It starts there using machine learning to block.

In [68], authors have designed a DDoS attack detector for Software Defined Network (SDN) architecture to be deployed in the POX controller. According to the results obtained in the simulation environment, their proposed model has achieved an accuracy of about 99.4%. This level of accuracy is much higher and better compared to Decision Tree (DT), K-Nearest Neighbor (KNN), and Support Vector Machine (SVM) approaches.

In [69], the main goal of this article is to improve the performance of the entire SDN network and they have proposed an algorithm that has been evaluated in the shortest path simulation environment and greedy routing algorithms by Java. The obtained results show that the algorithm proposed in this article has improved performance and cost metrics including utilization, delay, jitter, packet loss ratio (PLR), blocking probability (BP) and link cost.

In [70], the authors have addressed the important and challenging issues of flow discrimination and optimal allocation of resources in providing network resources needed for each flow. In this paper, a model consisting of distinct network flow types and optimal allocation of resources based on flow classes is proposed. Applications are clustered into four groups according to their network resource requirements, and a deep network traffic analyzer is used for classification. In this model, the greedy algorithm is also used for the optimal allocation of resources. have developed the proposed model in Mininet with Pox controller in parallel with maximum utilization to prove the improvement of Quality of Service (QoS). Compared to Spanning Tree Protocol (STP) and Dynamic Adaptive Multipath Routing (DAMR), the model presented in this paper performs better in allocating network resources based on flow requirements and maximizes network utilization.

In [71], authors have proposed a model to predict the optimal path to minimize the average delay between the source and destination nodes in SDN. The proposed model is implemented in the controller. The proposed model routed the flows based on the collected information in the controller. It showed better behaviour compared with q-routing and shortest-path routing algorithms.

In [72], the authors proposed routing to optimize the throughput and utilization in optical network links while they improve the convergence time using deep reinforcement learning based-routing algorithm. They have worked on an optical transmission network (OTN) organized in software defined network (SDN) architecture.

In [73], the network digital twin (NDT) has been addressed and discussed. The authors indicated that machine learning (ML) is used in different components of NDT because it needs to discriminate, classify, and predicts accurately and fast. The paper surveyed the technologies and the future trend in NDT and its applications in the real world. The research papers are summarized in Table 2 and organized to express key words, tools, application scope, case study and evaluation results.

In [74], the authors surveyed the digital twins (DT) and their applications in the real world to extract the challenges and future direction in the industries. The in-depth insight related to DT has been collected and deduced in the review research. The limitation, challenges and future trends have been discussed to pave the way for the researchers working on DT applications in the industries. It directed those intending to work on various aspects of DT to apply in the industries.

According to reviewed and analyzed research papers mentioned above, the ML roadmap in SDN is shown in Fig. 4.

3.1 The ML-based Solutions Categories in SDN

In accordance with the reviewed papers, it was deduced that each of the studies has worked on the improvement of one or more non-functional parameters. The papers' improvements are categorized based on non-functional improvement targets: reliability-aware, scalability-aware, performance-aware, balancing-aware, and hybrid. Table 3 shows the non-functional targets which have been used as the goal of improvement.

3.2 The Evaluation Parameters Used by the Research Papers

The proposed approaches in the research papers have been evaluated based on the metrics which are important for the researchers; thus, in this subsection, the papers are organized based on evaluation metrics and are shown in Table 4. The evaluation parameters extracted from the reviewed papers are performance optimization, security, platform provisioning, attack reduction, attack detection and load balancing metrics which have been used for the research solution evaluation.

3.3 The Evaluation Environment Used by the Research Papers

ML has three key phases which are training, evaluation, and test phases. The training phase is done based on the training set. The supervised learning model needs to be trained based on the dataset that had been labelled. The unsupervised model does not need to be trained with the labelled dataset. The semi-supervised learning is based on the data set in which a part of it is labelled while the other part is not labelled. According to the reviewed papers, the datasets which have been used for model creation in the ML model usage in SDN are KDD 99, CMU, TIET [8], CIC-DDOS 2019 [27] [26], INSDN [34], CICDOS 2017 [63]. The research papers' models have been evaluated in

Table 2 The brief of research papers based on subject, keywords, tools, application scope, case study and evaluation results

Article	Main subject	Key words	Tools	Scope of application	Case Study	Evaluation results
[3]	Routing Optimization in SDN by Investigating ML Techniques	Software-defined networking, machine learning, routing, optimization, and survey	ML techniques	Performance optimization	Supervised learning, unsupervised learning, and reinforcement learning	There is a great tendency to use intelligent routing in programmable networks
[7]	Automatic formation of flow law using ML in network software based on edge computing	Software-defined-network controller machine learning flow rule OpenFlow auto rule formation	Machine learning algorithms	Load balancing	A radiation software-defined network	Improving the network through software
[8]	Multimedia social security and finding suspicious activity on SDN using DL	Social multimedia; Software-defined networks; Flow routing; Deep learning; Anomaly detection;	An anomaly detection scheme based on blended deep learning	Security	CMU-based de-in-the-interior dataset	The mode and efficient control of the network by limiting the specific features such as energy-conscious networks and securing the execution time in the networks is enhanced by the software
[9]	Managing SDN flow log by boosting the flow	Design, algorithms, experimentation, performance	Traditional RL algorithm and deep RL	Load balance	Use Mininet	Shows an improvement of about 60% in the reduction of long-term control overhead and about a 14% increase in the impact-to-table ratio compared to the Bloom Multiple Filters (MBF) methods according to the fixed-size flow table of 4 KB
[10]	ML-based ransomware detection using SDN	ransomware; malware; software-defined networking; machine learning; stream processing; programmable forwarding engines	New hardware-based stream generators, RaftLib parallel framework	Security	Unencrypted characteristics of HTTPS traffic	A stream-based fingerprinting method to capture ransomware before encryption is feasible and accurate
[11]	SDN-based architecture to mitigate DDOS attacks using ML	DDoS attack mitigation, low-rate DDoS (LR-DDoS) attacks, machine learning, software-defined network (SDN)	A stream processor with five cores is written to process rich stream records	Attack mitigation and attack detection	New hardware-based stream generators in combination with the high-performance parallelism framework RaftLib	A detection accuracy rate of approximately 87% was achieved, while a strong false negative rate of nearly 10% was maintained
[3]	Dynamic clustering of SDN switches and controller placement using ML	deep learning techniques, Software-defined networking, multiple controllers	Mathematical model	Performance optimization	Dynamic clustering and placement based on deep Q network (DDCP)	By using the ONOS controller, the network performance can be significantly improved in terms of response time and resource utilization

Table 2 (continued)

Article	Main subject	Key words	Tools	Scope of application	Case Study	Evaluation results
[12]	Securing networks using SDN and ML	Software-defined networking; supervised learning; traffic classification; secure networks	A test platform based on Mininet	Security	Ixia Perfect Storm traffic simulator	Resource usage and traffic classification overhead are manageable, adding only 13% additional memory overhead and 17% CPU overhead compared to the same system without classification overhead
[13]	Detection and classification of conflict flows in SDN using ML	Software-defined network, conflict flow detection, flow classification, and machine learning algorithms	Decision Tree (DT), Support Vector Machine (SVM), Very Fast Decision Tree (EFDT), and Hybrid (DT-SVM)	Security	Streams were selected from 1000 streams to 100,000 streams with an incremental step of 10,000 streams for variable data sets	he proposed the EFDT algorithm obtained the best results compared to DT, SVM, and DT-SVM algorithms with a detection accuracy of 99.49%. Regarding the classification between conflict flow types, it has been proposed that EFDT achieved an accuracy of 95.73%
[14]	Evaluation of ML techniques for security in SDN	SDN; Security; IDS; DDoS; Machine Learning; Security in SDN	ML techniques	Security	Data set in the simulated environment	Three of the four algorithms have more than 96% accuracy, while SVM reached 97.5%. It also did not mix high bandwidth usage with a DDoS attack
[15]	BrainChain An ML approach to secure blockchain applications using SDN	DDoS; DNS Amplification; SDN; Bayes Classifier; Entropy; Blockchain	BrainChain	Security	Blockchain and FS scheme	BrainChain can quickly and effectively detect and mitigate attacks (i.e. DNS amplification attacks) with high accuracy and a small false positive rate
[16]	SDN intelligent traffic classification using DL	SDN, deep learning, big data, traffic analysis, traffic classification, and network management	A DL model called DEEP-SDN	Load balancing	Real-world traffic dataset	Deep-SDN performs better, reporting 96% overall accuracy
[17]	Detecting distributed denial of service attacks in SDN using ML	Security, Distributed Denial of Service (DDoS), Machine Learning (ML), SDN, SVM, Decision Tree	SVM and decision tree algorithm	Detection of attacks	KDD99 dataset	SVM with the decision tree technique performs better in the simulated environment. In this model, the accuracy increased to 96%

Table 2 (continued)

Article	Main subject	Key words	Tools	Scope of application	Case Study	Evaluation results
[18]	ML-based QOE prediction in SDN networks	SDN; Machine learning; prediction; estimation, accuracy	Decision tree (DT), neural network, K nearest neighbour KNN and Random Forest RF, Pearson correlation coefficient r and Root-Mean Square-Error RMSE	Providing the platform	DCR (degradation class classification)	It describes the environment based on the following: Weka is suitable for analyzing ML algorithms, MSU tools for calculating SSIM and VQM, and Mininet for SDN simulation
[19]	DRL-aware resource allocation in SDN-enabled fog paradigm	Deep reinforcement learning · Ofoading · Scheduling · Fog · Cloud · DQBRA ·SDN	A new container-based architecture with different fog nodes	Performance optimization	Software Define Network (SDN)	Q-network-based resource allocation innovates deep learning that performs up to 30% better on application costs (energy and execution time)
[20]	Reducing attacks in networks with SDN	network security, machine learning, reinforcement learning, software-defined networking, network function virtualization	Two machine learning algorithms	Reduce attacks	Virtual network	The proposed approach can be applied to reduce the impact of attacks on a small private network
[21]	Predicting network attack patterns in SDN using ML	Network Attack; Machine Learning; Honeypots, SDN	C4.5, Bayesian network (Bayes Net), decision table (DT), and simple	Detection of attacks	Network attack data	Machine learning algorithms can help define security rules for the SDN controller, and a prediction accuracy of 91.68% was achieved with the Bayesian network
[22]	Identification of DDOS attacks through ML and SDN statistical methods	Distributed denial-of-service attacks · Software-defined networks · Highvolume DDoS attack · Low-volume DDoS attack · Network security	Collector, entropy-based algorithms, and classification	Detection of attacks	UNB-ISCX, CTU-13, and ISOT datasets	The accuracy of this proposed method is higher than other similar methods
[23]	Attack pattern prediction through ML using the firewall in the SDN network	software-defined network; network function virtualization; firewall; SDNFV; attack prediction; machine learning; decision table; bayesian network	Stateful firewall as VNF in SDN network	Detection of attacks	Normal network data (DT), Bayesian network algorithms (Bayes Net), Naive-Bayes, C4.5, and decision table (DT)	The decrease in prediction accuracy with an increasing threshold indicates that the smallest possible attack threat should not be ignored, and the firewall security policies in the stateful VNF firewall module should be changed to reject the potential threat

Table 2 (continued)

Article	Main subject	Key words	Tools	Scope of application	Case Study	Evaluation results
[24]	ML-based attack detection and mitigation system for IOT with SDN	Internet of Things; Distributed Denial-of-Services; network security; software-defined networking; adaptive machine learning; detection; mitigation	Support Vector Machine (SVM), Naive Bayes (NB), Random Forest (RF), k-Nearest Neighbor (KNN), and Logistic Regression (LR) classifications	Attack detection, attack mitigation	Simulation environment	The simulation results validate the intelligent DDoS detection and mitigation framework of AMLSDM for real-time network traffic classification generated by two IoT networks with SDN
[25]	Detecting and mitigating DDOS attacks in SDN using ML	SDN, DDoS, Machine Learning, J48, Weka	، K-NN، J48 و Random Forest	Attack detection, attack mitigation	Online data	J48 is the most suitable classifier for the network considered by the authors of the article
[26]	ML analysis for securing SDN	Distributed Denial of Service (DDoS) Attack; Machine Learning Algorithm; Security; Software-Defined Networking (SDN)	ML-based designs	security	CIC-DDoS 2019	XGBoost can detect DDoS attacks on SDN with low accuracy, recall, F1 score, and error
[27]	ML-based multipath routing for SDN	Machine learning · Software-defined networks · Software-defined networking · Routing	Network state estimates and their corresponding routing settings in the network's central controller	Performance optimization	Real network traffic data	Performance evaluation of the MLMR framework on real network traffic traces confirms its accuracy and robustness against noise in the training data. Furthermore, the MLMR framework shows more than 98.99% improvement in computational efficiency
[28]	Miners' reputation management in blockchain based on ML and SDN	Blockchain · Distributed trust model · Miner reputation · Signaling games · Machine learning · Software Defined networks	Labour market signalling model, trust model parameters	Performance optimization	Simulation environment	The PoolCoin blockchain provides a trust model that protects the mining pool from misbehaving miners
[29]	Detection of security anomalies in SDN	SDN, OpenFlow, Anomaly detection, Data plane, Security challenges, Virtual networks	ML algorithms	security	Statistical data	The machine learning method is much more suitable for detecting an abnormality than other methods because they are more comprehensive and accurate than other methods

Table 2 (continued)

Article	Main subject	Key words	Tools	Scope of application	Case Study	Evaluation results
[30]	Deep Place is a DL for implementing adaptive flow rules in software-defined IoT networks	Flow rule placement Quality-of-Service Software-Defined Networking Internet of Things Deep reinforcement learning	The process of transporting traffic in an SDIoT network Markov Decision Process (MDP) with continuous action space	Providing the platform	Network traffic data	DeepPlace can efficiently maintain a significant number of race fields in a flow rule while minimizing the QoS violation ratio of the traffic flow and keeping the flow tables in the switches under their maximum flow
[31]	A load balancer-based DL for network intrusion detection in SDN sensors	Software-defined networking (SDN)، Network performance Intelligent, Load Balancing, Autonomous, Security	Mechanism-based on convergence	Load balancing	Advanced intrusion detection datasets	The load balancing mechanism can achieve 2 × performance improvement compared to traditional methods
[32]	A QoS-aware traffic classification architecture using ML and deep packet inspection in SDNs	traffic classification, QoS, machine learning, SDN	DPI and multi-class semi-supervised learning	Performance optimization	Real network traffic data	The proposed architecture can implement efficient traffic classification with high accuracy
[33]	Vehicle data loading by roadside units using intelligent SDN	Road-Side Unit, Software Defined Network, Reinforcement Learning, Mobile Edge Computing;	SRDO Algorithm, Q-Learning	Load balancing	Urban environment data	The reduction of package loss percentage by 9% has shown a noticeable difference. This improvement affects overall network performance by increasing network throughput and reducing latency
[34]	DL to detect Denial of Service attacks in SDN	Software-Defined networking (SDN); Denial of Service (DoS); Deep Learning (DL); Recurrent Neural Networks (RNN); LongShort-Term Memory (LSTM); Gated Recurrent Unit (GRU);	DL algorithms	Detection of attacks	In SDN dataset	Increased accuracy to detect Denial of Service (DoS) attacks
[35]	ML-based load balancing for multiple controllers in SDN	Software-Defined Network (SDN), Controller load balancing, Deep Reinforcement Learning (DRL), Switch immigration	Markov Decision Process (MDP),	Load balancing	Simulation environment	DRL-SMS can effectively balance the controller load and reduce the balancing time significantly

Table 2 (continued)

Article	Main subject	Key words	Tools	Scope of application	Case Study	Evaluation results
[36]	ML-based SDN controller for drone management	Radiofrequency, Support vector machines, Machine learning algorithms, Distributed Ledger, Authentication, Delays, Classification Algorithms	ML algorithms include decision trees (DT), random forest (RF), support vector machine (SVM), and logistic regression (LR)	Performance optimization	drone	The RF algorithm shows the best performance with an accuracy of 92.81% in UAV-type classification
[37]	Native SDN intrusion detection using ML	software-defined networking, SDN, intrusion detection, deep learning, autoencoder, network security	An unsupervised hybrid machine learning approach	security	Deployed model for throughput and latency	The proposed module has a minimal overhead on SDN controller performance while providing very high detection accuracy
[38]	Content popularity and caching for ICN an ML approach with SDN	Information-centric networking, SDN, deep learning, content popularity prediction, the caching scheme	SAE architecture, implementation of neuron functionality in an SDN switch, and DLCPP deployment in an OpenFlow-based SDN	Providing the platform	Softmax classifier	By benefiting from the better predictive accuracy of DLCPP, CPC can consistently improve cache performance over other dominant cache management frameworks
[39]	Routing in optical networks based on SDN with the help of ML	Machine-Learning-based, software-defined networks	Traffic matrices	Performance optimization	Optimal routing historical traffic tracking	This module can classify traffic matrices to provide real-time routing decisions
[40]	Energy-Efficient Traffic-Aware Routing in SDN in ML Framework	Machine-Learning-based, software-defined networks	Mininet and POX controller	Providing the platform	real environment	Umin and Umax prediction accuracy is more than 70%. The heuristic refinement algorithm converges to the optimal values of Umin and Umax 15 to 25 times faster than the brute force method
[41]	Hybrid DL is an efficient detection and monitoring mechanism in SDN	Security, hybrid deep learning model, software-defined networks, long short-term memory, convolutional neural network	Hybrid DL-based architecture with Cuda capability	Performance optimization	CICIDS2017 dataset and standard performance evaluation criteria	In terms of detection accuracy, it performs with a negligible speed trade-off
[42]	ML-based load balancing model and sector routing in SDN	software-defined networks, load balancing, segment routing, machine learning	Algorithms and load-balancing mechanisms	Load balancing	Static and dynamic load balancing	This model improves QoS and provides the ability to predict the overload of network paths
[16]						In this model, the accuracy increased to 96%

Table 2 (continued)

Article	Main subject	Key words	Tools	Scope of application	Case Study	Evaluation results
[17]		Security, Distributed Denial of Service (DDoS), Machine Learning, Software-defined network (SDN), Support Vector Machine (SVM), Decision Tree				
[43]	Detection of DDOS attack on SDN control plane using ML techniques	Software Define Network, Machine Learning(ML), Hybrid Machine learning, DDoS, SVM, Self-Organized Map (SOM)	SVM and SOM algorithm	Detection of attacks	Three performance measures such as accuracy, detection rate, and false alarm rate were studied	Compared to simple machine learning models, this model offers lower accuracy, detection rate, and false alarm rate
[44]	Traffic data classification using ML algorithms in SDN	Machine learning, supervised learning, automatic network data classification, ONOS	ML algorithms	Performance optimization	ML algorithms	Machine learning algorithms can effectively classify network traffic data
[45]	ML in SDN	Machine Learning, Software Defined Networks, SDN	Supervised, unsupervised learning	Performance optimization	Intent-Based Networking (IBN)	Learning or semi-supervised learning methods help to solve some specific problems in SDN
[46]	Security risk assessment for smart networks with SDN	Cyber Resilience; Smart Grid; SDN; Security Metrics; OpenFlow; IED	Security risks of DoS attacks on intelligent electronic devices (IED) and IEC 61850 network	security	IED device	Network SDN frees the smart grid from congestion and improves the scheduling performance of IEC 61850-type messages and makes them time-sensitive
[47]	Performance analysis of SDN-based prevention in cyberspace phishing attack using DL with CANTINA approach (DMLCA)	Software Define Network, Phishing attack, DMLCA approach, text classifier, information retrieval algorithm, performance analysis, hyperlinks, support vector machine	SVM technique	Providing the platform	(TF) and inverse document frequency (IDF)	This method is an effective way to predict a phishing attack in cyberspace
[48]	SDN-based DL-based intelligent malware detection for the Internet of Medical Things (IoMT)	Deep learning (DL), Internet of Things (IoT), Internet of Medical Things (IoMT), Factory-of Things (FoT), Hybrid Deep Learning, Architecture, Executable Malware, SDN	Hybrid architectures based on DL	Security	Publicly available datasets	IoMT's sophisticated malware detection performs better for subsequent mitigation and prevention

Table 2 (continued)

Article	Main subject	Key words	Tools	Scope of application	Case Study	Evaluation results
[49]	IPro: An approach to SDN intelligent monitoring	Knowledge-Defined Networking, Machine Learning, Probing Interval, Software-Defined Networking, Traffic Monitoring	An architecture based on a knowledge-defined network paradigm, a reinforcement learning-based algorithm, and an IPro prototype	Providing the platform	Reinforcement Learning to determine the exploration distance	IPro is an efficient approach for Moni's SDN regarding CCO, CCU, and MA
[50]	PrePass-Flow: An ML-Based Technique to Minimize ACL Policy Violations Due to Link Failures in Hybrid SDN	Hybrid SDN, Machine Learning, ACL, Link Failure Prediction, Network Reachability	Both the SDN wizards model and legacy switches model	Providing the platform	access control (ACL)	The LR model outperforms both the SVM model and the existing approach in terms of packet delivery ratio (PDR) and ACL policy violation
[51]	Intelligent routing mechanism with QoS guarantee in software-defined networks	SDN, IoT, Data flow classification and QoS are guaranteed to route	Data stream classification called MACCA2-RF&RF	Performance optimization	Local routing algorithm	Simulation results show that MACCA2-RF&RF can efficiently classify data streams with a recognition accuracy of 99.73%, and QI-RM can guarantee the QoS requirements of data streams before and after link congestion
[52]	The secure architecture of objects with DL and SDN	Internet of Things -Software-defined networks -Anomalies detection-Deep learning, Restricted-Boltzmann Machine	Restricted Boltzmann Machines (RBM)	Performance optimization	Simulation environment	It represents the overall integration of IoT and SDN to increase security by up to 94%
[53]	DRL-R: A DL Approach for Intelligent Routing in Software Defined Data Center Networks	Deep Reinforcement Learning, Routing, Network Resource, SDN, Data Center Networks	Deep Q Network (DQN) and Deep Deterministic Policy Gradient (DDPG)	Providing the platform	DRL-R compared to OSPF	DDPG performs better than DQN
[54]	A GRU deep learning system against attacks in software-defined networks	Gated recurrent units- SDN, Deep Learning, DDoS, Intrusion Detection	Gated Recursive Units (GRU) deep learning method	Detection of attacks	Public datasets, CICDDoS 2019 and CICIDS 2018	The results indicate high detection rates and a high amount of analyzed streams per second, which makes GRU a practical approach for the proposed system

Table 2 (continued)

Article	Main subject	Key words	Tools	Scope of application	Case Study	Evaluation results
[55]	Flow-based anomaly intrusion detection using ML with software-defined networking for the OpenFlow network	Anomaly Intrusion -Detection, Machine Learning Model, Multi-layer Classification, Network Traffic, OpenFlow, Packet Data Flow, QoS, SDN	Data packets through the network and virtual circuits	Security	Priority based algorithm	Compared with the traditional methods, the proposed work is compared with the existing schemes in the network to produce results with fast routing and fault tolerance of the existing networks to overcome the open gap in the security of the SDN architecture to identify and identify the vulnerabilities
[56]	A multi-user service migration scheme based on deep reinforcement learning and SDN in mobile edge computing	Mobile edge computing Container migration Multi-user mobility Deep reinforcement learning Aware delay Energy consumption	Traditional RL and base algorithms, DRLMSM	Providing the platform	MEC environment	Our proposed DRLMSM can achieve better performance, and the DRLMSM-DDQN sub-algorithm can achieve the best performance
[57]	An ML-based SDN model for the Internet of Things: an incremental tensor train approach	Deep Boltzmann Machine, Network Intelligence, Software Defined Networking, Tensor Train Decomposition	Order-based generalization mechanism called tensor	Providing the platform	Deep Boltzmann machine and incremental tensor train decomposition model	The proposed architecture outperforms its conventional counterpart in terms of throughput, latency, and storage space considering the variation in the number of traffic flows, table occupancy index, request rate, and several flow entries
[58]	Adaptive and reliable communications with SDN capability in IoT-Fog environment using machine learning and multi-objective optimization	Fog computing, Internet of Things (IoT), machine learning (ML), multiobjective optimization (MOO), software-defined networks (SDNs)	MOO algorithm	Performance optimization	ML-based algorithm in a software-enabled multihop (SDN) scenario for IoT-fog environment	1) the trade-off between these two objectives can be optimized and 2) the SDN controller can make an adaptive decision to choose the best path among the paths
[59]	Deep learning-based slow DDoS attack detection in SDN-based networks	Slow DDoS Attack, Software-Defined Networking, Deep Learning, Performance Evaluation, Supervised Learning	Multilayer Perceptron (MLP) and standard machine learning models and Class 1 Support Vector Machines (Class 1 SVM)	Attack detection	Custom datasets	The combined CNN-LSTM model has a high performance of 99% compared to other algorithms

Table 2 (continued)

Article	Main subject	Key words	Tools	Scope of application	Case Study	Evaluation results
[60]	Deceiving machine learning-based saturation attack detection systems in SDN	software-defined networking, adversarial attacks, DoS saturation attacks, machine learning-based detection systems	Saturation attacks (SYN, UDP, ICMP, and TCP-SARFU),	Attack detection	Different supervised and unsupervised machine learning classifiers	The proposed adversarial testing tool can effectively compromise machine learning-based saturation attack detection systems
[61]	Identification of deep learning approach and defence against DDoS attacks in SDN environments	Adversarial attacks-DDoS-Deep Learning-GAN-SDN	Generative Adversarial Network (GAN)	Attack detection	Simulated data and CICD-DoS 2019 public dataset	The proposed system effectively detects up-to-date types of DDoS attacks compared to other approaches
[62]	ML and Software-Defined Networking for Secure Communications in Crowds of Drones	FANET-SDN-AODV Security architecture-Machine Learning-Random Forest Classifier	Random forest classification	Performance optimization	OpenFlow events	The proposed detection model has a good F1 score, although with a small detection delay
[63]	SDN-based architecture for application layer DDoS attack detection using ML, DL	Software-defined networking, deep learning, machine learning, DDoS attack, transport layer, application layer, slow-rate attacks	Mininet Network Simulator and Open Network Operating System (ONOS) SDN Controller	Attack detection	CICDoS2017 and CICD-DoS2019 datasets	Detection rate above 98% for transport DDoS attacks and up to 95% for application layer DDoS attacks
[64]	Collaborative intrusion detection for VANETs: a distributed SDN approach based on deep learning	Collaborative intrusion detection, intelligent transportation, distributed SDN, deep learning, and generative adversarial networks	Vehicle Ad hoc Network (VANET)	security	Real-world dataset	The proposed CIDS is efficient and effective in intrusion detection for VANET
[65]	ABRAHAM: ML-based active forwarding algorithm using SDN	IEEE 802.11, SDN, handover algorithm	Alternative handover algorithms in IEEE 802.11, SDN, handover algorithm	Performance optimization	Software Defined Network (SDN) called HuMOR	There is a statistically significant difference between ABRAHAM and other algorithms
[66]	SDN preemptive load balancing with ML for delay-sensitive applications	Load balancing, machine learning, migration, multi-access edge computing, predictions, reinforcement learning, and software-defined networking	Autoregressive integrated moving average (ARIMA) and long-term short-term memory (LSTM) approaches	Load balancing	simulation	The proposed algorithm performs close to optimal and performs better than the recent benchmark algorithms from the literature

Table 2 (continued)

Article	Main subject	Key words	Tools	Scope of application	Case Study	Evaluation results
[67]	The concept of intelligent detection of DDoS attacks in SDN networks using ML	Measurement, Machine learning algorithms, Databases, Web services, Machine learning, Denial-of-service attacks, IP networks	Kullback–Leibler approach	Attack detection	Server access times from IP addresses	2WSLS has near-optimal performance and outperforms benchmark algorithms in terms of load balance and migration cost
[68]	DDOS attack detection accuracy improvement in software defined network (SDN) using ensemble classification	computer crime, computer network security, Internet, pattern classification, software defined networking, telecommunication traffic	DDoS attack discriminator, POX controller	Attack detection	a DDoS attack discriminator will be designed for Software Defined Network (SDN) architecture	accuracy of about 99.4%, which shows a significant improvement compared to the Decision Tree (DT), K-Nearest Neighbor (KNN), and Support Vector Machine (SVM) approaches
[69]	A novel flow routing algorithm based on non-dominated ranking and crowd distance sorting to improve the performance in SDN	Software-defined network (SDN), Flow routing algorithm, Performance, Multi-objective Optimization	Java greedy routing algorithms	Performance optimization	shortest path and greedy-based routing algorithms will be simulated by Java	The proposed optimization algorithm improves all performance metrics such as utilization, delay, jitter, packet loss ratio (PLR), blocking probability (BP) and link cost simultaneously
[70]	Automatic delay-sensitive applications quality of service improvement with deep flows discrimination in software defined networks	SDN, Traffic classification, Deep learning, Network Utilization	Deep network traffic detector, greedy algorithm	Performance optimization	Simulation	The proposed model behaves intelligently in allocating network resources based on flow requirements compared to Spanning Tree Protocol (STP) and Dynamic Adaptive Multipath Routing (DAMR) while maximizing network utilization
[71]	GraphNET: Graph Neural Networks for routing optimization in Software Defined Networks	Routing algorithm, destination nodes, deep reinforcement learning, Graph Neural Networks, packet delay	Controller	Performance optimization	various small and large topologies	The proposed algorithm shows impressive results when compared to q-routing and shortest path routing algorithm in terms of the above experiments and is robust to the varying graphical structure of the network
[72]	A routing optimization method for software-defined optical transport networks based on ensembles and reinforcement learning	optical transport network; software-defined networking; deep Q-network; message-passing neural network; ensemble learning	Deep reinforcement learning (DRL)- and software-defined networking (SDN)	Performance optimization	message passing neural network (MPNN)-based DRL policy network	EMDQN effectively improves the throughput rate and link utilization of optical networks and has better generalization capabilities

Table 2 (continued)

Article	Main subject	Key words	Tools	Scope of application	Case Study	Evaluation results
[73]	Network Digital Twin: Context, Enabling Technologies, and Opportunities	Network topology, Optimization, Delays, Analytical Models, Topology, Computational Modeling, Digital Twins	the architecture of the NDT, modern machine learning (ML)	Performance optimization	QoS-aware, ML-based NDT	describe the general architecture of the NDT and argue that modern machine learning (ML) technologies enable building some of its core components
[74]	Digital Twins: A Survey on Enabling Technologies, Challenges, Trends and Future Prospects	Digital twins, Tutorials, Internet, Market research, Solid modelling, Monitoring, Data Visualization	DTs	Performance optimization	Industry, infrastructure and healthcare	This survey article aims to cover important aspects of the realization of technology. Key technologies, challenges and prospects for DTs are highlighted

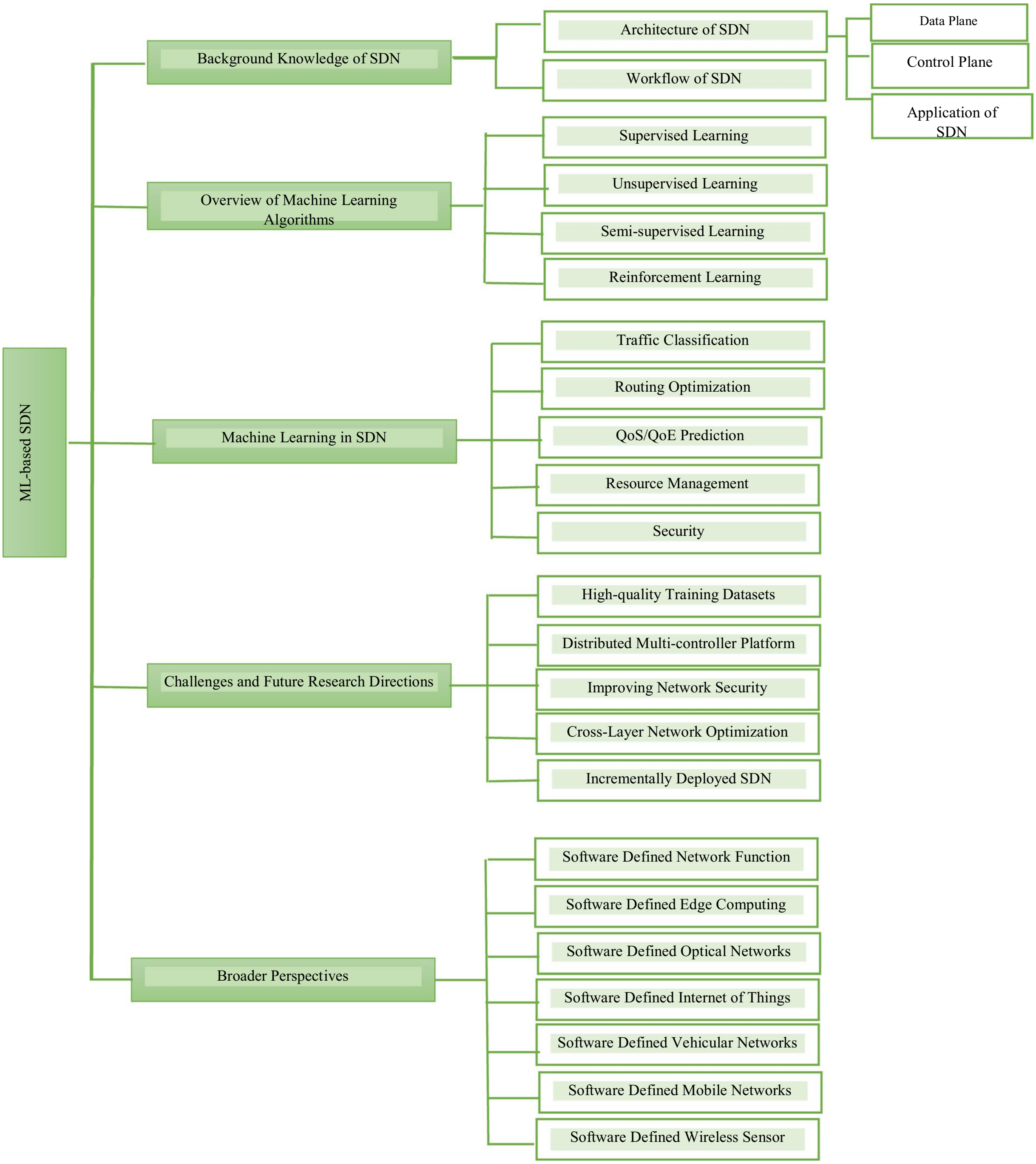
ML-based SDN
Background Knowledge of SDN
Architecture of SDN
Workflow of SDN
Data Plane
Control Plane
Application of SDN
Overview of Machine Learning Algorithms
Supervised Learning
Unsupervised Learning
Semi-supervised Learning
Reinforcement Learning
Machine Learning in SDN
Traffic Classification
Routing Optimization
QoS/QoE Prediction
Resource Management
Security
Challenges and Future Research Directions
High-quality Training Datasets
Distributed Multi-controller Platform
Improving Network Security
Cross-Layer Network Optimization
Incrementally Deployed SDN
Broader Perspectives
Software Defined Network Function
Software Defined Edge Computing
Software Defined Optical Networks
Software Defined Internet of Things
Software Defined Vehicular Networks
Software Defined Mobile Networks
Software Defined Wireless Sensor

Fig. 4 Tree view of ML in SDN

different environments extracted from the papers. These evaluation environments are real environment, prototype, simulation, algorithmic model, and hybrid model. Therefore, the papers are categorized based on these evaluation environments in Table 5.

4 Discussion and Future Direction

In this section, the reviewed papers will be discussed to extract the research gap and trend for those working on ML in SDN. The quantity analysis of the papers will result in the following outcomes for the solutions, evaluation

Table 3 Solutions Clustering

Article	Solution Category				
	Reliability-aware	Scalability-aware	Performance-aware	Load balancing-aware	Hybrid
[7]			✓		
[8]	✓			✓	
[9]					
[10]			✓		
[11]					✓
[3]			✓		
[12]	✓				
[13]					✓
[14]	✓				
[15]	✓				
[16]				✓	
[17]	✓				
[18]			✓		
[19]			✓		
[20]	✓				
[21]	✓				
[22]					✓
[23]					✓
[24]	✓				
[25]	✓				
[26]	✓				
[27]		✓			
[28]			✓		
[29]	✓				
[30]			✓		
[31]				✓	
[32]				✓	
[33]				✓	
[34]					✓
[26]	✓				
[35]				✓	
[36]			✓		
[3]					✓
[37]	✓				
[38]			✓		
[39]			✓		
[40]					✓
[41]					✓
[42]				✓	
[16]			✓		
[17]	✓				
[43]	✓				
[44]			✓		
[45]			✓		
[46]	✓				
[47]	✓				
[48]	✓				
[49]	✓				
[50]					✓
[51]			✓		
[52]	✓				
[53]			✓		
[54]	✓				
[55]	✓				
[56]			✓		
[57]		✓			
[58]					✓
[59]	✓				
[60]			✓		
[61]	✓				
[62]	✓				
[63]					✓
[64]	✓				
[65]		✓			
[66]				✓	
[67]	✓				
[68]	✓				
[69]			✓		
[70]			✓		
[71]			✓		
[72]					✓
[73]			✓		
[74]					✓

parameters and evaluation environment for the ML models proposed for usage in SDN architecture.

4.1 Discussion

The research papers have utilized ML to improve the network's non-functional parameters, so the proposed solutions need to be aware of the network situation to improve the ML model with feedback. These model awareness can be grouped into reliability, scalability, performance, and load-balancing. There are some models which are trained based on multi-awareness which is called 'hybrid'.

According to the number of research papers that addressed each of the solutions, the pie chart in Fig. 5 is presented.

As shown in Fig. 5, the reliability-aware solutions are paid more attention by the researchers working on ML in SDN with 46%. The second highest priority of the researchers belongs to performance-aware solutions with 25%. The

Table 4 research papers clustering based on Evaluation Parameters

Article	Evaluation Parameters					
	Performance optimization	security	Platform provisioning	Attacks		Load balancing
				Attack reduction	Attack detection	
[7]						✓
[8]		✓				
[9]						✓
[10]		✓				
[11]				✓	✓	
[3]	✓					
[12]		✓				
[13]		✓				
[14]		✓				
[15]		✓				
[16]						✓
[17]					✓	
[18]			✓			
[19]	✓					
[20]				✓		
[21]					✓	
[22]					✓	
[23]					✓	
[24]				✓	✓	
[25]				✓	✓	
[26]		✓				
[27]	✓					
[28]	✓					
[29]		✓				
[30]			✓			
[31]						✓
[32]	✓					
[33]						✓
[34]					✓	
[26]		✓				
[35]						✓
[36]	✓					
[3]	✓					
[37]		✓				
[38]			✓			
[39]	✓					
[40]			✓			
[41]	✓					
[42]						✓
[16]	✓					
[17]					✓	
[43]					✓	
[44]	✓					
[45]	✓					
[46]		✓				
[47]			✓			
[48]		✓				

Table 4 (continued)

Article	Evaluation Parameters					
	Performance optimization	security	Platform provisioning	Attacks		Load balancing
				Attack reduction	Attack detection	
[49]			✓			
[50]			✓			
[51]	✓					
[52]	✓					
[53]			✓			
[54]					✓	
[55]		✓				
[56]			✓			
[57]			✓			
[58]	✓					
[59]					✓	
[60]					✓	
[61]					✓	
[62]	✓					
[63]					✓	
[64]		✓				
[65]	✓					
[66]						✓
[67]					✓	
[68]					✓	
[69]	✓					
[70]	✓					
[71]	✓					
[72]	✓					
[73]	✓					
[74]	✓					

hybrid, load-balancing, and scalability-based solutions with 16%, 10% and 3% are the other priorities, respectively.

The evaluation parameters are the other aspects which have been examined in this paper. The Fig. 6 shows the percentage of research papers which have been evaluated in different ways: performance optimization, security, platform provisioning, attack reduction, attack detection, and load-balancing.

According to Fig. 6, the highest percentage related to the performance optimization parameters was 29% and belongs to performance optimization. The second evaluation parameters which have been used by the researchers are attack detection with 23%. Security, platform provisioning, load-balancing, and attack reduction are the next parameters which have been used for the evaluation of the proposed ML model for SDN.

Figure 7 shows the used environment in the research papers which can help those simulating or implementing their model for SDN research. The environments used for evaluation in each research paper are categorized into five sections: real environment, Algorithmic method, Simulation, Prototype, and hybrid environment.

Based on Fig. 7, the researchers have worked on ML in SDN in different environments. Most number of papers have worked with the algorithmic method which 30% of papers have used it. The second highest evaluation environment has been the hybrid environment with 20%. Also, 17% of studies were evaluated in SDN simulation environments like Mininet. 13% of the papers have utilized prototypes for the evaluation of the environment. The research papers which used the real environment are only 20%.

4.2 Future Research Directions

According to the reviewed papers, the research papers have worked on SDN to improve the non-functionalities like network performance, security, reliability and quality of services. In this trend, the major models belong to supervised learning. The researchers intend to train their model based on the collected dataset. The researchers used the simulation

Table 5 Research papers clustering based on experiment environments

Article	Experiment Environment				
	Hybrid model	Algorithmic model	Simulation	Prototype	Real environment
[7]			✓		
[8]			✓		
[9]			✓		
[10]	✓				✓
[11]		✓			✓
[3]	✓				
[12]	✓	✓			
[13]		✓			
[14]			✓	✓	
[15]	✓				✓
[16]					✓
[17]		✓	✓		
[18]		✓			
[19]				✓	✓
[20]		✓			
[21]		✓			
[22]		✓			
[23]		✓			
[24]			✓		
[25]				✓	
[26]				✓	
[27]					✓
[28]			✓		
[29]		✓			
[30]	✓				
[31]		✓			
[32]					✓
[33]		✓			
[34]		✓			
[26]		✓			
[35]			✓		
[36]		✓			
[3]	✓				
[37]					✓
[38]	✓				
[39]	✓				
[40]					✓
[41]	✓				
[42]		✓			
[16]					✓
[17]		✓			
[43]	✓				
[44]		✓			
[45]				✓	
[46]					✓
[47]			✓		
[48]	✓				
[49]				✓	
[50]	✓				
[51]		✓			
[52]					✓
[53]			✓		
[54]			✓		
[55]					✓
[56]		✓			
[57]	✓				
[58]	✓				
[59]	✓				
[60]				✓	
[61]				✓	
[62]				✓	
[63]			✓		
[64]					✓
[65]		✓			
[66]			✓		
[67]				✓	
[68]			✓		
[69]		✓			
[70]	✓				
[71]		✓			
[72]		✓			
[73]					✓
[74]					✓

to prove the performance and application of their proposed model. Most proposed models have been trained for reactive use cases. This trend refers to the deficiencies that exist in the feedback and response time. In the following, the future research direction will be discussed.

The research papers analysis shows that the researchers have worked on reliability to improve performance, security, and attack detection. The researchers proposed the ML-based model for online improvement in SDN. The proposed model needs to get feedback on the network status to optimize the ML-based model. To monitor and check the status of the network for reliability, performance, and load balancing, the metrics like delay, throughput, jitter, blocking probability, and others have been collected with different sensors, but scalability is a problem in SDN because its assessment is difficult. The scalability assessment metrics can evaluate the software defined networks' scalability status is a challenging

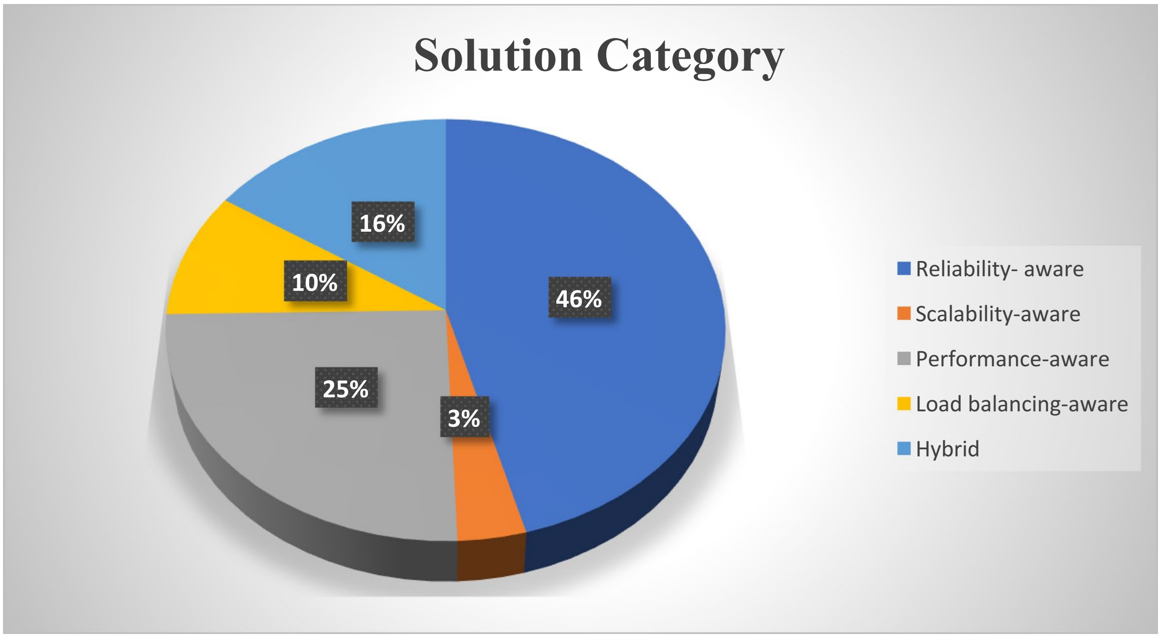

Fig.5 The research papers solutions classification

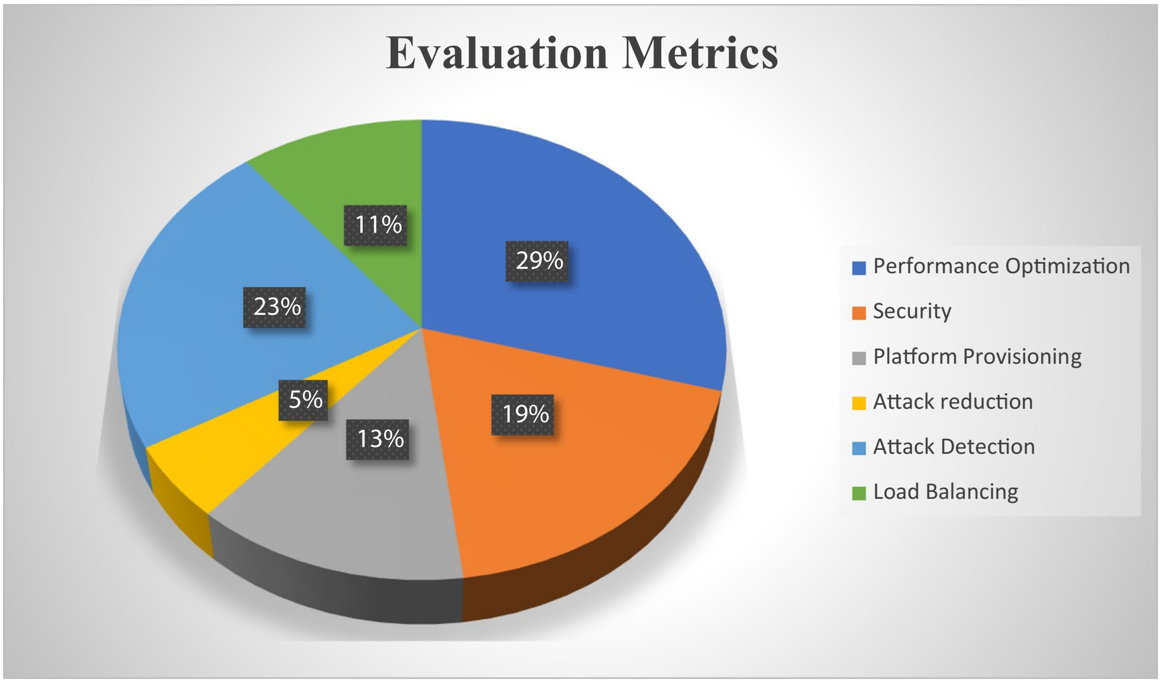

Fig.6 The research paper evaluation classification

issue and gap which can be used by the researcher working on SDN and ML.

According to the research analysis, there are a few papers which have worked on the routing function, which is a fundamental one, using a graph neural network (GNN) approach to improve the other non-functional parameters such as QoS, security, etc. The routing function is centralized in the SDN, and it is not different, whether physical or conceptual centralized control plane. SDN programmability and network topology, which are based on graphs naturally, can motivate the researcher to use GNN for future research on SDN and ML. Most papers have used GNN for topology

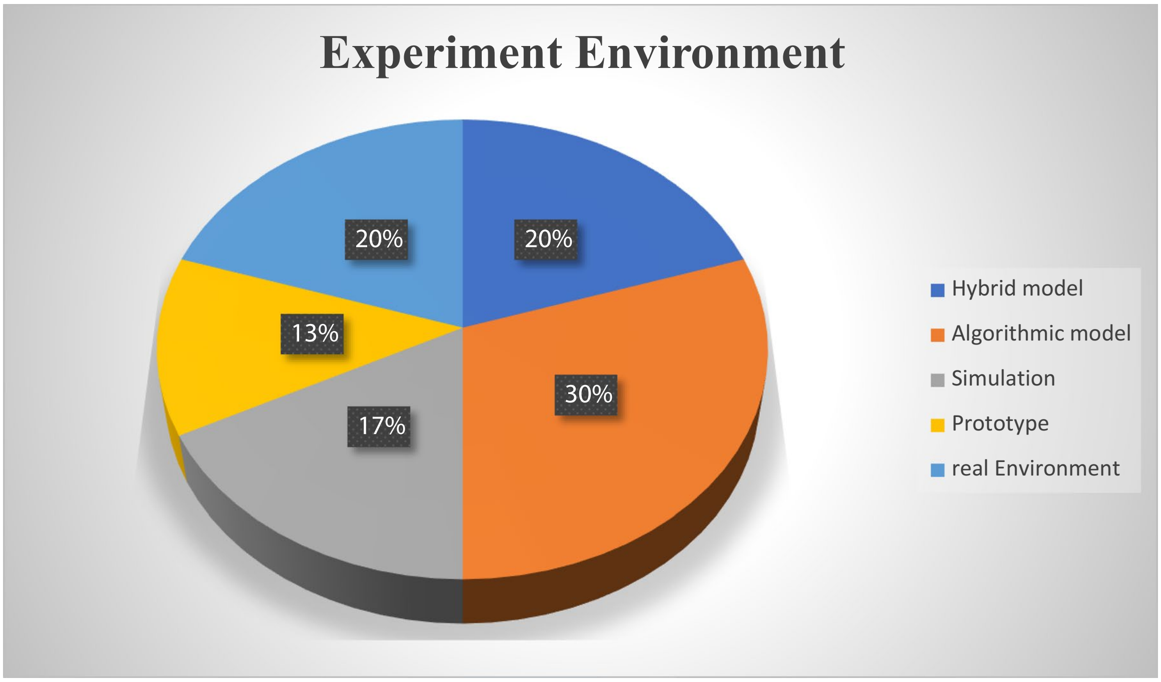

Fig. 7 The research papers experiments' environment classification

extraction and routing, therefore it can be used in the routing to improve or optimize other non-functional parameters not addressed so far, moreover, it can even be used for topology prediction in networks whose topology is changing such as vehicular ad-hoc networks (VANET), Mobile ad-hoc networks (MANET), etc.

The research papers' quantity and quality assessments indicate that most approaches are based on online reactions like attack detection, or identification while there is a gap for the research based on proactive models which are needed for the design purpose to prevent attack, failure, performance, and quality reduction. The proactive ML-based model is the other direction for future research. The other challenge which can be addressed is the online learning that is used in the reactive models to grow the model, it will be a big challenge because there is no short-term feedback for model performance improvement and the proactive model depends on the consequences of designs which take a long time. The online learning model in this proactive model causes another challenge which can be addressed in future research works.

The digital twin is a concept which needs nearly zero-delay live traffic, which is a challenging issue. To guarantee the network resource allocation, network traffic extraction is required which is a current challenge and there are some pieces of research which addressed this on accuracy and delay. Although SDN has made the network programmable and flexible, its (physical and conceptual) centralized architecture can be a challenge because can increase the delay compared with traditional networks. These challenges next to the other digital twin requirements which should be provided with the network control layer in SDN are the future research direction. The digital twin application in SDN can be a hot topic in 6G with which researchers have been currently dealing.

Most papers have used simulation to evaluate their trained models, and it is required for the researcher to evaluate their proposed model in a real environment. In addition, online learning in a real environment can improve security gradually. The ML-based model for reactive security which is trained online is the other research gap which can be examined in future research works. The real environment is less paid attention to in the research papers we examined.

5 Conclusion

Nowadays, the growth of Internet coverage and complexity has caused the SDN to have emerged. SDN has made the network more programmable and flexible. On the other hand, machine learning is the other trend which has been making the systems more intelligent. Therefore, in this survey, we examined the research papers that addressed ML and SDN. The research papers published in Springer, Elsevier, IEEE and ACM which have addressed different forms and derivations of ML and SDN between 2016 and 2023 were considered. The research issues, solutions, evaluation parameters, and environments have been examined and the research papers clustered. According to the quantity and quality assessments done in this paper, the research topics were discussed and the future research directions have been stated in this review paper. In accordance with the reviewed papers analysis, most papers have addressed the reactive model to detect and identify using SDN, architecture thus, the proactive model which is used by the designers to mitigate future issues is a prominent gap in the recent research papers related to ML and SDN. This proactive Ml-based model can be used in SDN but online learning which improves itself by feedback is difficult because the response time in this type of ML-based model is long. Online learning can improve the model performance which is significant with using a real environment that has not been used in the reviewed papers. This survey is useful for those working on SDN and ML and can help them to move through the research direction related to ML and SDN.

Author contributions Sahar collected the papers and Alireza observed the collection and writing the paper.

Funding There is no funding for this paper.

Availability of data and material Not Applicable.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Shirmarz A, Ghaffari A. Performance issues and solutions in SDN-based data center: a survey. J Supercomput. 2020;76(10):7545–93.
2. Xie J, Richard YuF, Tao H, Renchao X, Jiang L, Chenmeng W, Yunjie L. A survey of machine learning techniques applied to software-defined networking (SDN): Research issues and challenges. IEEE Commun Surv Tutor. 2018;21(1):393–430.
3. Amin R, Elisa R, Aqsa A, Sadia R, David C-P, Jose MA. A survey on machine learning techniques for routing optimization in SDN. IEEE Access. 2021.
4. Ebneyousef S, Alireza S. A taxonomy of load balancing algorithms and approaches in fog computing: a survey. Cluster Comput. 2023: 1–22.
5. Mohammadi R, Akleylek S, Ghaffari A, Shirmarz A. Taxonomy of traffic engineering mechanisms in software-defined networks: a survey. Telecommun Syst. 2022;81(3):475–502.
6. Jiang W. Graph-based deep learning for communication networks: a survey. Comput Commun. 2022;185:40–54.
7. Iqbal S, Hira M, Kashif NQ, Ibrahim TJ, Noel C. Automated flow rule formation by using machine learning in software-defined networks based edge computing. Egypt Inform J. 2022;23(1):149–57.
8. Chen JIZ, Smys S. Social multimedia security and suspicious activity detection in SDN using hybrid deep learning technique. J Inform Technol. 2020;2(02):108–15.
9. Mu T-Y, Al-Fuqaha A, Shuaib K, Sallabi FM, Qadir J. SDN flow entry management using reinforcement learning. ACM Trans Autonom Adapt Syst (TAAS). 2018;13(2):1–23.
10. Cusack G, Oliver M, Eric K. Machine learning-based detection of ransomware using SDN. In: Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, pp. 1–6. 2018.
11. Perez-Diaz JA, Ismael AV, Kim-Kwang RC, Dakai Z. A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning. IEEE Access. 2020;8:155859–72.
12. Comaneci D, Ciprian D. Securing networks using SDN and machine learning. In: 2018 IEEE International Conference on Computational Science and Engineering (CSE), pp. 194–200. IEEE. 2018.
13. Khairi MHH, Sharifah HSA, Nurul MAL, Kamaludin MY, Mohamed KH, Fahad TA-D, Mosab H, Suleman K, Muzaffar H. Detection and classification of conflict flow in SDN using machine learning algorithms. IEEE Access. 2021;9: 76024–76037.
14. Ahmad A, Erkki H, Mika Y, Ijaz A. Evaluation of machine learning techniques for security in SDN. In: 2020 IEEE Globecom Workshops (GC Wkshps, pp. 1–6. IEEE. 2020.
15. Abou EH, Zakaria AH, Lyes K. BrainChain-A machine learning approach for protecting blockchain applications using SDN. In: ICC 2020–2020 IEEE International Conference on Communications (ICC), pp. 1–6. IEEE. 2020.
16. Malik A, Ruairí DF, Mohammed A-Z, Javier A-P. Intelligent SDN traffic classification using deep learning: Deep-SDN. In: 2020 2nd International Conference on Computer Communication and the Internet (ICCCI), pp. 184–189. IEEE. 2020.
17. Sudar KM, Beulah M, Deepalakshmi P, Nagaraj P, Chinnasamy P. Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques. In: 2021 International Conference on Computer Communication and Informatics (ICCCI), pp. 1–5. IEEE. 2021.
18. Abar T, Asma BL, Sadok EA. Machine learning based QoE prediction in SDN networks. In: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 1395–1400. IEEE. 2017.
19. Lakhan A, Mazin AM, Omar IO, Chinmay C, Karrar HA, Seifedine K. Efficient deep-reinforcement learning aware resource allocation in SDN-enabled fog paradigm. Automat Softw Eng. 2022;29(1):1–25.
20. Zolotukhin M, Sanjay K, Timo H. Reinforcement learning for attack mitigation in sdn-enabled networks. In: 2020 6th IEEE Conference on Network Softwarization (NetSoft), pp. 282–286. IEEE. 2020.
21. Nanda S, Faheem Z, Casimer DC, Eric W, Baijian Y. Predicting network attack patterns in SDN using machine learning approach. In: 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pp. 167–172. IEEE. 2016.

22. Banitalebi D, Afsaneh MRS, Farsad ZB. The DDoS attacks detection through machine learning and statistical methods in SDN. J Supercomput. 2021;77(3):2383–415.
23. Prabakaran S, Ramalakshmi R, Irshad H, Balasubramanian PK, Sultan SA, Ahmed SA, Abdullah A. Predicting attack pattern via machine learning by exploiting stateful firewall as virtual network function in an SDN network. Sensors. 2022;22(3):709.
24. Aslam M, Dengpan Y, Aqil T, Muhammad A, Muhammad H, David N, Samia AC, Mohamed AE, Mohammed AAA-Q, Syeda FJ. Adaptive machine learning based distributed denial-of-services attacks detection and mitigation system for SDN-Enabled IoT. Sensors. 2022;22(7): 2697.
25. Rahman O, Mohammad AGQ, Chung-Horng L. DDoS attacks detection and mitigation in SDN using machine learning. In: 2019 IEEE world congress on Services (SERVICES), vol. 2642, pp. 184–189. IEEE. 2019.
26. Alamri HA, Thayananthan V. Analysis of machine learning for securing software-defined networking. Proc Comput Sci. 2021;194:229–36.
27. Awad MK, Marwa HHA, Ali FA, Imtiaz A. Machine learning-based multipath routing for software-defined networks. J Netw Syst Manag. 2021;29(2):1–30.
28. Kaci A, Rachedi A. Toward a machine learning and software-defined network approaches to manage miners' reputation in the blockchain. J Netw Syst Manage. 2020;28(3):478–501.
29. Jafarian T, Masdari M, Ghaffari A, Majidzadeh K. A survey and classification of the security anomaly detection mechanisms in software-defined networks. Clust Comput. 2021;24(2):1235–53.
30. Nguyen TG, Trung VP, Dinh TH, Hai HN, Duc TL. DeepPlace: Deep reinforcement learning for adaptive flow rule placement in Software-Defined IoT Networks. Comput Commun. 2022;181:156–63.
31. Ahmed U, Lin J-W, Srivastava G. A resource allocation deep active learning based on the load balancer for network intrusion detection in SDN sensors. Comput Commun. 2022;184:56–63.
32. Yu C, Lan J, Xie JiChao, Yuxiang Hu. QoS-aware traffic classification architecture using machine learning and deep packet inspection in SDNs. Proc Comput Sci. 2018;131:1209–16.
33. Guntuka S, Shakshuki EM, Yasar A, Gharrad H. Vehicular data offloading by roadside units using the intelligent software-defined network. Proc Comput Sci. 2020;177:151–61.
34. Alshraa AS, Ahmad F, Jochen S. Deep learning algorithms for detecting denial of service attacks in software-defined networks. Procedia Comput Sci. 2021;191:254–63.
35. Xiang M, Mengxin C, Duanqiong W, Zhang L. Deep reinforcement learning-based load balancing strategy for multiple controllers in SDN. e-Prime-Adv Elect Eng Electron Energy 2022;2: 100038.
36. Yazdinejad A, Elnaz R, Ali D, Reza MP, and Gautam S. A machine learning-based sdn controller framework for drone management. In: 2021 IEEE Globecom Workshops (GC Wkshps), pp. 1–6. IEEE. 2021.
37. Isa MM, Lotfi M. Native SDN intrusion detection using machine learning. In: 2020 IEEE Eighth International Conference on Communications and Networking (ComNet), pp. 1–7. IEEE. 2020.
38. Liu W-X, Zhang J, Liang Z-W, Peng L-X, Cai J. Content popularity prediction and caching for ICN: a deep learning approach with SDN. IEEE Access. 2017;6:5075–89.
39. Troia S, Alberto R, Ignacio M, José AH, Oscar GDD, Rodolfo A, Francesco M, Guido M. Machine-learning-assisted routing in SDN-based optical networks. In: 2018 European Conference on Optical Communication (ECOC), pp. 1–3. IEEE. 2018.
40. Assefa BG, Oznur O. MER-SDN: Machine learning framework for traffic-aware energy-efficient routing in SDN. In: 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing, and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), pp. 974–980. IEEE. 2018.
41. Malik J, Adnan A, Iram B, Muhammad I, Arslan M, Sung WK. Hybrid deep learning: An efficient reconnaissance and surveillance detection mechanism in SDN. IEEE Access. 2020;8:134695–706.
42. Todorov D, Hristo V, Veneta A. Load balancing model based on machine learning and segment routing in SDN. In: 2020 International Conference Automatics and Informatics (ICAI), pp. 1–4. IEEE. 2020.
43. Deepa V, Muthamil Sudar K, Deepalakshmi P. Detection of DDoS attack on SDN control plane using hybrid machine learning techniques. In: 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 299–303. IEEE. 2018.
44. Kwon J, Daeun J, Hyunggon P. Traffic data classification using machine learning algorithms in SDN Networks. In: 2020 International Conference on Information and Communication Technology Convergence (ICTC), pp. 1031–1033. IEEE. 2020.
45. Liu J, Qiaozhi X. Machine learning in a software-defined network. In: 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), pp. 1114–1120. IEEE. 2019.
46. Maziku H, Shetty S, Nicol DM. Security risk assessment for SDN-enabled smart grids. Comput Commun. 2019;133:1–11.
47. Ravi R. A performance analysis of Software Defined Network based prevention on phishing attack in cyberspace using a deep machine learning with CANTINA approach (DMLCA). Comput Commun. 2020;153:375–81.
48. Khan S, Akhunzada A. A hybrid DL-driven intelligent SDN-enabled malware detection framework for Internet of Medical Things (IoMT). Comput Commun. 2021;170:209–16.
49. Castillo EF, Rendon OMC, Ordonez A, Granville LZ. IPro: An approach for intelligent SDN monitoring. Comput Netw. 2020;170:107108.
50. Ibrar M, Wang L, Muntean G-M, Akbar A, Shah N, Malik KR. PrePass-flow: a machine learning based technique to minimize ACL policy violation due to links failure in hybrid SDN. Comput Net. 2021;184:107706.
51. Sun W, Wang Z, Zhang G. A QoS-guaranteed intelligent routing mechanism in software-defined networks. Comput Netw. 2021;185: 107709.
52. Dawoud A, Shahristani S, Raun C. Deep learning and software-defined networks: towards secure IoT architecture. Internet Things. 2018;3:82–9.
53. Liu W-X, Jun C, Qing CC, Yu W. DRL-R: Deep reinforcement learning approach for intelligent routing in software-defined data-center networks. J Netw Comput Appl. 2021;177:102865.
54. Assis MVO, Luiz FC, Jaime L, Mario LP Jr. A GRU deep learning system against attacks in software defined networks. J Netw Comput Appl. 2021;177: 102942.
55. Satheesh N, Rathnamma MV, Rajeshkumar G, Vidya Sagar P, Pankaj D, Dogiwal SR, Priya V, Sudhakar S. Flow-based anomaly intrusion detection using machine learning model with software-defined networking for OpenFlow network. Microprocessors Microsyst. 2020;79:103285.
56. Chen W, Chen Y, Jiaxing Wu, Tang Z. A multi-user service migration scheme based on deep reinforcement learning and SDN in mobile edge computing. Phys Commun. 2021;47: 101397.
57. Singh A, Gagangeet SA, Sahil G, Georges K, Gurpreet S. Deep-learning-based SDN model for the Internet of Things: an incremental tensor train approach. IEEE Internet Things J. 2019;7(7):6302–11.
58. Akbar A, Muhammad I, Mian AJ, Ali KB, Lei W. SDN-enabled adaptive and reliable communication in IoT-fog environment using machine learning and multiobjective optimization. IEEE Internet Things J. 2020;8(5):3057–65.

59. Nugraha B, Rathan NM. Deep learning-based slow DDoS attack detection in SDN-based networks. In: 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pp. 51–56. IEEE. 2020.
60. Khamaiseh, Samer Y., Izzat Alsmadi, and Abdullah Al-Alaj. "Deceiving machine learning-based saturation attack detection systems in sdn." In 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pp. 44–50. IEEE, 2020.
61. Novaes MP, Luiz FC, Jaime L, Lemes Proença M. Adversarial Deep Learning approach detection and defence against DDoS attacks in SDN environments. Fut Gen Comput Syst. 2021;125:156–67.
62. Guerber C, Royer M, Larrieu N. Machine learning and software defined network to secure communications in a swarm of drones. J Inform Secur Appl. 2021;61: 102940.
63. Yungaicela-Naula NM, Cesar V-R, Jesus AP-D. SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning. IEEE Access 2021;9: 108495–108512.
64. Shu J, Zhou L, Zhang W, Xiaojiang Du, Guizani M. Collaborative intrusion detection for VANETs: a deep learning-based distributed SDN approach. IEEE Trans Intell Transp Syst. 2020;22(7):4519–30.
65. Zeljković E, Slamnik-Kriještorac N, Latré S, Marquez-Barja JM. ABRAHAM: machine learning backed proactive handover algorithm using SDN. IEEE Trans Netw Serv Manage. 2019;16(4):1522–36.
66. Filali A, Mlika Z, Cherkaoui S, Kobbane A. Preemptive SDN load balancing with machine learning for delay-sensitive applications. IEEE Trans Veh Technol. 2020;69(12):15947–63.
67. Klymash M, Olga S, Nazar P, Oksana M. Concept of intelligent detection of DDoS attacks in SDN networks using machine learning. In: 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), pp. 609–612. IEEE. 2020.
68. Shirmarz A, Ali G, Ramin M, Sedat A. DDOS attack detection accuracy improvement in software defined network (SDN) using ensemble classification. In: 2021 International Conference on Information Security and Cryptology (ISCTURKEY), pp. 111–115. IEEE. 2021.
69. Shirmarz A, Ghaffari A. A novel flow routing algorithm based on non-dominated ranking and crowd distance sorting to improve the performance in SDN. Photon Netw Commun. 2021;42:167–83.
70. Mohammadi R, Akleylek S, Ghaffari A, Shirmarz A. Automatic delay-sensitive applications quality of service improvement with deep flows discrimination in software defined networks. Clust Comput. 2023;26(1):437–59.
71. Swaminathan A, Mridul C, Deepak KS, Uttam G. GraphNET: graph neural networks for routing optimization in software defined networks. Comput Commun. 2021;178: 169–182.
72. Chen J, Xiao W, Li X, Zheng Y, Huang X, Huang D, Wang M. A routing optimization method for software-defined optical transport networks based on ensembles and reinforcement learning. Sensors. 2022;22(21):8139.
73. Almasan P, Miquel F-G, Jordi P, José S-V, Diego P, Diego L, Antonio APP, et al. Network digital twin: context, enabling technologies, and opportunities. IEEE Commun Mag. 2022;60(11):22–7.
74. Mihai S, Mahnoor Y, Dang VH, William D, Praveer T, Mohsin R, Mehmet K, et al. Digital twins: a survey on enabling technologies, challenges, trends and future prospects. IEEE Commun Surv Tutorials. 2022.