Iraqi Journal of Communications and Computer Networks
e-ISSN: 3105-9252, p-ISSN: 3105-9244
Vol. (1), Iss. (1), September 2025
DOI: https://doi.org/10.58564/IJCCN.1.1.2025.2

https://ijccn.net/ **Research Article**

Integrating Machine Learning in Software-Defined Networks: A Comprehensive Survey

Mohammad Khalid [1*], Hassan Mohamed Muhialdeen [2]

[1] Department of Computer Engineering, College of Engineering, Al-Iraqia University, Iraq
Email: mohammad.k.abass@aliraqia.edu.iq
[2] Department of Computer Engineering, College of Engineering, Al-Iraqia University, Iraq
Email: muhialdeen.hassan@aliraqia.edu.iq
***Corresponding Author:** muhialdeen.hassan@aliraqia.edu.iq

Citation: Mohammad Khalid, & Hassan Mohamed Muhialdeen. (2025). Integrating Machine Learning in Software-Defined Networks: A Comprehensive Survey . Iraqi Journal of Communications and Computer Networks (IJCCN), (00), 14–19.

ARTICLE INFO

Received: 14 Apr. 2025
Revised: 26 Jun. 2025
Accepted: 09 Jul. 2025

ABSTRACT

As we know the Internet became an important part of our daily life, as the fast increasing spread of the Internet and technologies nowadays is resulting in a more varied and complicated network. Through the network separation between the control plane and the data plane where software-defined networking (SDN) has transformed the network architecture. The systems have become more Intelligence thanks in part to machine learning (ML) and the rest of its branches. Machine learning and SDN have been subjects of several academic publications. This survey compiles research articles published in Springer, Elsevier, IEEE, ACM on the issue of SDN &ML (2018 - 2023). Research is structured according to solutions, evaluation criteria, and evaluation environments so that SDN and ML teams have the greatest opportunity of optimizing the intended non-functional and functional qualities. This review paper will gather the results of the analyses of the researchers to extract environments, assessment criteria, and solutions. This paper will discuss future areas of research and the research deficit.

Keywords: software defined, network (SDN),artificial intelligence, Machine learning (ML),Deep learning,Deep reinforcement learning.

INTRODUCTION

The Internet's diversity and complexity are driving the need for a new network design as its reach and quality continue to grow at a dizzying rate. The software-defined network (SDN)[1] demonstrates that the modern network needs to be programmable, elastic, and flexible. With the data plane and control plane now physically separated, the network is much more flexible and easy to program thanks to the SDN design. In order to simplify the network, this architecture makes use of a central controller. These designs consist of three layers: data, control, and application. On top of that, it works with three different APIs: one for each direction (north, south, east, and west). You may see the SDN's design in Figure 1. In order to link the control layer with the application layer, the northbound API is used. In order to link the control and data layers, the southbound API is used. To make SDN more scalable and to expand the control layer, the authors propose the eastbound and westbound APIs. Their role in enabling controller connections and dispersed controller formation—also known as conceptual central controllers as opposed to actual central controllers [1] stands as the rationale for this. However, the system's intelligence has been enhanced thanks to machine learning (ML), which has granted it the ability to make decisions. One place where this capacity may be utilized in SDN is the control layer, which is responsible for making decisions in the architecture. [1]. Machine learning has enhanced SDN's nonfunctional concepts like network performance, security, and quality of service. Supervised, unsupervised, semi-supervised, and reinforcement learning are the four primary subfields of ML [2]. Since ML has been suggested for various uses

and improvement goals in numerous SDN research articles, we sift through the most recent articles to identify the goals for improvement and solutions that have been proposed.

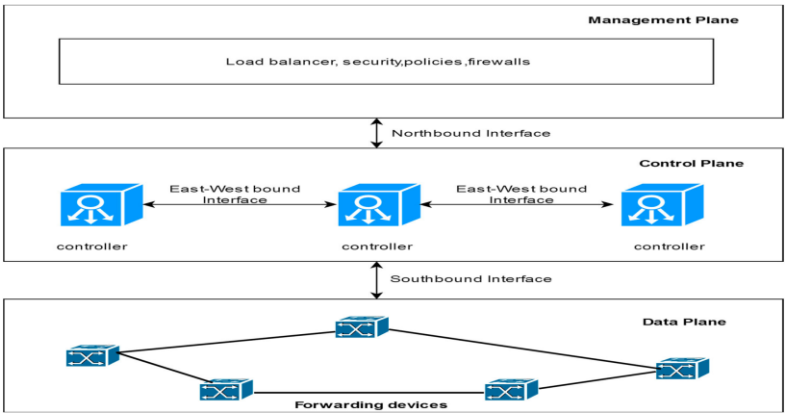

Figure 1: Software-Defined Network Architecture[3]

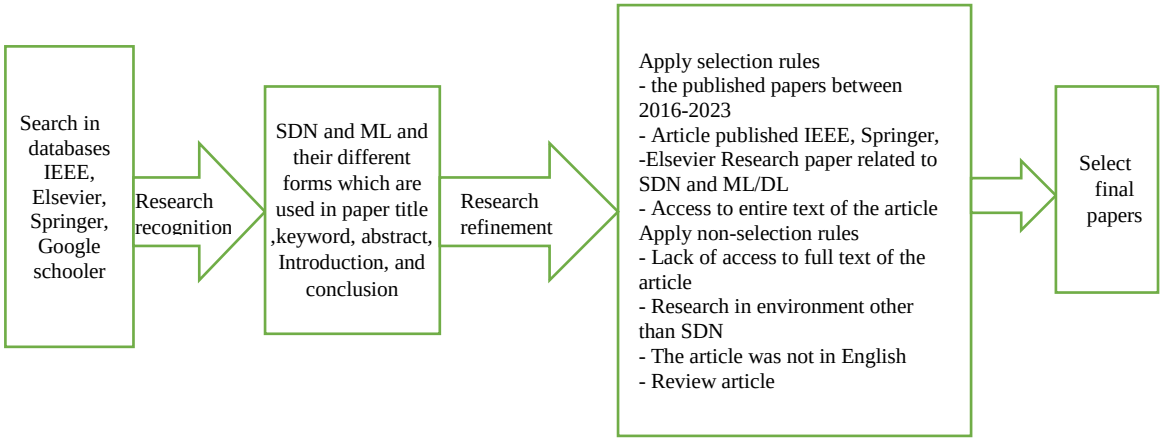

Figure 1 : standards for choosing research articles

This survey is beneficial for researchers who are working on SDN to improve the non-functional aspects using ML, as it demonstrates the research deficit and future prospects associated with SDN in the context of ML. This survey proceeds according to the procedures illustrated in Figure 2: searching, identifying papers, evaluating, enhancing research, selecting articles, and developing articles.

LITERATURE REVIEW

Due to the rapid development of technology, the network has become more complex in terms of the basic architecture of the network, resources and devices. Machine learning was a challenge in closed networks in the past, but through SDN, the flexibility and programmability of the network has increased. This has contributed to exploiting the multiple capabilities of the network, as machine learning has become able to improve network functions such as performance, security, etc. Because of SDN, machine learning consists of a model, parameters and a learning system. If the model makes a prediction, the parameters increase the prediction or classification. The learning system trains the model, evaluates it and tests it through training and test sets.

With the application layer decoupled from the controller, this article zeroes in on the problem of missing flow rules as it pertains to packet loss and latency in an SDN context. in which Within the conventional software-defined networking (SDN) controller, the authors propose a new sub-module called a Rule Formation Agent (RFA). An essential part of efficient network traffic management is the

RFA's use of reinforcement learning to automate the creation of flow rules. Throughput, packet loss ratio, and latency are all enhanced by the suggested solution.[4] in this paper, the researchers address the problem of managing flow entries, as the number of nodes in the network increases, the number of forwarding rules also increases more than the capacity of the triple content memory, where when the permissible limit is reached, the switches stop accepting messages from the controller, which leads to unnecessary traffic in the control plan and delays in processing packets and delays, and this occurs due to the coexistence of long-lived (elephant) and short-lived (mice) flows .the paper utilizes traditional and deep reinforcement learning algorithms within a Markov Decision Process framework to optimize flow entry management in SDN, focusing on reducing control overhead and improving packet forwarding efficiency. The results indicate a significant improvement of around 60% in reducing long-term control overhead and a 14% increase in the table-hit ratio compared to the Multiple Bloom Filters (MBF) method, given a fixed size flow table of 4KB.[5] The security issues caused by the ever-increasing volume of social multimedia traffic are the focus of this article. The article focuses on problems like data breaches and identity theft that occur because personal information is so easily accessible and because social networks have so much data. Attacks such as account hijacking, phishing, impersonation, and malware distribution have increased alongside the spread of multimedia material throughout social media platforms, as pointed out by the authors. Effective management and analysis of social multimedia information requires the creation of scalable and widespread communication paradigms that preserve sufficient security levels By integrating two primary deep learning methods—Supported Boltzmann Machines (RBMs) and Support Vector Machines (SVMs)—this research introduces a new framework for protecting social multimedia traffic. Software Defined Networks (SDNs) rely on these methods to identify suspicious behavior and outliers.[6] The problem addressed in this research is the detection and mitigation of ransomware, especially in the area of advanced malware delivery. Many ransomware detection techniques have relied on deep packet inspection (DPI) to analyze network traffic, with a particular focus on HTTP traffic. Due to the shift of malware delivery to HTTPs that encrypt the payload, traditional methods have become ineffective. Measurements of interarrival time and input/outflow length rank first through eight among the authors' ransomware traffic classification criteria. Using these eight criteria, a random forest model is trained to classify ransomware. Tenfold cross-validation guarantees that the model is unbiased, and the data is split into a training set consisting of 70% and a testing set consisting of 30%. Classifier performance in detecting malware is 0.87 F1 score, 0.83 accuracy, and 0.89 recall.[7] In order to protect SDN systems from low-rate distributed denial-of-service (LR-DDoS) attacks, the authors conducted research and proposed a modular, adaptable design. Because of the architectural separation of detection and mitigation, the Intrusion Detection System (IDS), which requires a lot of processing power, can be located outside of the SDN controller, where it can better manage the network's resources. With a detection rate of 95% and low false alarm rates, the IDS identifies malicious or benign network flows using machine learning models such as J 48, Randomtree, REPtree, Random Forest (RF), multi-layer perception (MLP), & the support vector machine (SVM). The modular design of the framework makes it easy to add or remove elements, which increases its flexibility & scalability.[8] The authors have investigated sophisticated network security and explained how machine learning with SDN might be used to provide such security. Among these procedures are anomaly detection, botnet awareness, and honeypot rerouting. They are learning operational techniques. Complex network systems and their current solutions have been distributed, scaled, and architecturally based on SDN machines and controlled.[9] A novel deep-learning model for software-defined networks, known as Deep-SDN, has been put forth. In a brief amount of time, our model can reliably identify a large variety of traffic applications. The suggested model's performance has been contrasted with the state-of-the-art in this domain. The investigations' findings show that the proposed model is more effective in terms of F-score, accuracy, and recall. An overarching level of precision of 96% can be attained with the suggested model.[10] Researchers in this study used a method called decision-tree (DT) and support-vector machine (SVM) to detect malicious traffic. Many in the machine learning community classify this method as one of their own. After conducting experiments, it was found that the suggested approach outperforms the alternatives in terms of detection rate and accuracy.[11] In order to address the issue of resource allocation in heterogeneous fog networks that are geographically dispersed, a new container-based architecture that incorporates a variety of fog nodes has been developed. Deep learning is a skill that may be achieved through the utilization of this architecture. Allocation of resources for Q-network-based systems Finding a solution to the problem of resource allocation, which is comprised of multiple components[12] To improve network security and scalability, one solution is to (virtualize a software-

defined network function, SDNFV). This study positions stateful firewall services inside the SDN network as virtual network functions (VNFs). To prevent potentially harmful network connections, the SDN controller establishes regulations and guidelines.[13] To help reduce assaults, the researchers have developed an attack detection and mitigation system based on flexible machine- learning, which they call AMLSDM. Using an adaptive ML classification model, the AMLSDM system efficiently identifies and mitigates DDoS assaults. It is a safeguard for Internet of Things devices that can employ SDN capabilities.[14] this paper's authors proposed One approach to centralizing multi-path routing in SDNs is the MLMR framework, which makes use of machine learning. It trains a deep neural network (DNN) with network status data and heuristic techniques, allowing for efficient and accurate routing decisions. Data Warehouse, Data Analytics and Training Management, Data Acquisition and Results Reporting, and ML-Based Routing are some of the components that make up the system. When contrasted with conventional heuristic algorithms, the MLMR structure show over a 98.99% enhancement in computing proficiency while maintaining good prediction accuracy. Network traffic characteristics impact the framework's effectiveness; datasets with strongly correlated traffic matrices yield improved prediction accuracy. In conclusion, multi-path routing for software-defined networks has come a long way thanks to the MLMR structure.[15] To address the imbalance in demand on the control plane of many controllers, a deep reinforcement learning (DRL-SMS) switch migration strategy could be used. This method mimics SDN migration procedures and uses system incentives to decide the system state using a Markov decision process (MDP). By optimizing with Q-parameters, the Double- Deep Q-Network (DDQN) approximate function fitting is achieved using the Q-values of the switch migration action. The DDQN training network is enhanced via experience replay. Once trained, it takes the current system state's Q-value to determine DRL, and then it chooses the highest Q-value for switch migration. The suggested method improves controller load balance and reduces balancing time, according to simulations.[16]A control plane-based hybrid deep learning system is presented for effective detection of advanced cyber threats and attacks in software-defined networks. For high detection accuracy, the suggested technique combines LSTM and CNN predictive power. Control plane-based orchestration makes the hybrid deep learning framework scalable, versatile, and programmable, allowing it to be readily extended and modified to any commercial SDN controller. SDNs' centralized control plane is vulnerable to sophisticated cyberattacks, however this technique solves security issues. The suggested framework surpasses other deep learning-based algorithms in detection accuracy with a minimum trade-off in speed efficiency, according to thorough comparisons.[17] It has been suggested that an architectural paradigm can tackle the problem of load balancing in software-defined networks. By integrating segment routing with machine learning techniques, the proposed model achieves better performance and load balancing in the network. Improving QoS to allow prediction of network pathway overload is one of the main advantages of the proposed architectural paradigm.[18] After studying the approaches for attaining a guaranteed QoS for data flows, a smart routing method with a QoS guarantee, referred to as QI-RM in SDN, was suggested. Simulation findings show that the proposed mechanism works as expected: QI-RM meets data stream QoS requirements before and after link congestion, outperforming more traditional routing algorithms like ECMP and Dijkstra, and MACCA2-RF&RF efficiently classifies data streams with an identification accuracy of 99.73 percent.[19] In order to solve the problems associated with inefficient resource allocation, the authors of this study propose a DRL-R routing scheme for SD-DCN, or software-defined data center networks. Through the quantification of their contribution scores in lowering latency, DRL-R recombines numerous network resources with distinct metrics, including cache and bandwidth. The scheme constructs the DRL-R with the help of deep deterministic policy gradient (DDPG) and deep Q-network (DQN). Throughput, flow completion time, and link load balancing are all enhanced by DRL-R, according to the simulation results. The DRL-R routing system is another area where DDPG excels above DQN.[20] A new strategy for intelligent software-defined networks is the IoT-Train-Deep method. By employing an incremental tensor train decomposition model and a deep Boltzmann machine, the authors of this study have sought to integrate network intelligence into the flow transmission architecture of (SDN). Changes in request rate, number of flow entries, table occupancy index, and the amount of traffic flows have led to significant improvements in throughput, storage space, and delay in the suggested model.[21]

Categories of Machine- Learning-based Solutions in SDN

The papers that were reviewed led to the conclusion that all of the investigations focused on improving non-functional aspects. Depending on their focus on non-functional enhancement objectives, the papers' enhancements are classified

as either hybrid, scalability-aware, performance-aware, or reliability-aware. Table one displays the enhancement goals that are not functional.

Table 1: Solutions Clustering

Papers	Reliability - aware	Scalability - aware	Performance - aware	Load balancing aware	Hybrid
[4]			✓		
[5]	✓				
[6]	✓			✓	
[7]			✓		
[8]					✓
[9]	✓				
[10]				✓	
[11]	✓				
[12]			✓		
[13]					✓
[14]	✓	✓			
[15]		✓			
[16]				✓	
[17]					✓
[18]				✓	
[19]			✓		
[20]			✓		
[21]		✓			

Evaluating Factors Applied in Research Papers

In this part, the papers are classified according to assessment metrics and can be found in Table 2. The research articles' suggested methodologies have been assessed using the metrics that are essential to the researchers. For the purpose of evaluating the research solutions, the following assessment factors were taken from the papers that were reviewed: performance optimization, security, platform provisioning, attack minimization, attack detection, and load balancing metrics

Table 2: clustering of articles of research applying evaluation factors

Papers	Performance Optimization	Security	Platform pro-visioning	Attack Reduction	Attack Detection	Load balancing
[4]						✓
[5]						✓
[6]		✓				
[7]		✓				
[8]				✓	✓	
[9]		✓				
[10]						✓
[11]					✓	
[12]	✓					
[13]					✓	
[14]				✓	✓	
[15]	✓					
[16]						✓
[17]	✓					
[18]						✓
[19]	✓					
[20]			✓			
[21]			✓			

CONCLUSION

This research aims to review some research papers that employed machine learning in software-defined networks (SDN), Where we explained the problem of each research and the mechanism for solving it and we presented

Categories of Machine- Learning-based Solutions in SDN and Evaluating Factors Applied in Research Papers Which showed the result of the impact created by employing artificial intelligence (machine learning) in the SDN environment.

ETHICAL DECLARATION

Conflict of interest: No declaration required. **Financing:** No reporting required. **Peer review:** Double anonymous peer review.

REFERENCES

[1] A. Shirmarz and A. Ghaffari, *Performance issues and solutions in SDN-based data center: a survey*, vol. 76, no. 10. Springer US, 2020. doi: 10.1007/s11227-020-03180-7.

[2] J. Xie *et al.*, "A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 393–430, 2019, doi: 10.1109/COMST.2018.2866942.

[3] V. Srivastava, R. S. Pandey, and V. Srivastava, "Load balancing for software-defined network : a review," 2021, doi: 10.1080/1206212X.2021.1919835.

[4] S. Iqbal, H. Maryam, K. N. Qureshi, I. T. Javed, and N. Crespi, "Automised flow rule formation by using machine learning in software defined networks based edge computing," *Egypt. Informatics J.*, vol. 23, no. 1, pp. 149–157, 2022, doi: 10.1016/j.eij.2021.10.001.

[5] T. Y. Mu, A. Al-Fuqaha, K. Shuaib, F. M. Sallabi, and J. Qadir, "SDN flow entry management using reinforcement learning," *ACM Trans. Auton. Adapt. Syst.*, vol. 13, no. 2, 2018, doi: 10.1145/3281032.

[6] D. J. I. Z. Chen and D. S. S., "Social Multimedia Security and Suspicious Activity Detection in SDN using Hybrid Deep Learning Technique," *J. Inf. Technol. Digit. World*, vol. 2, no. 2, pp. 108–115, 2020, doi: 10.36548/jitdw.2020.2.004.

[7] G. Cusack, O. Michel, and E. Keller, "Machine learning-based detection of ransomware using SDN," *SDN-NFVSec 2018 - Proc. 2018 ACM Int. Work. Secur. Softw. Defin. Networks Netw. Funct. Virtualization, Co-located with CODASPY 2018*, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1145/3180465.3180467.

[8] J. A. Perez-Diaz, I. A. Valdovinos, K. K. R. Choo, and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning," *IEEE Access*, vol. 8, pp. 155859–155872, 2020, doi: 10.1109/ACCESS.2020.3019330.

[9] D. Comaneci and C. Dobre, "Securing networks using SDN and machine learning," *Proc. - 21st IEEE Int. Conf. Comput. Sci. Eng. CSE 2018*, pp. 194–200, 2018, doi: 10.1109/CSE.2018.00034.

[10] A. Malik and M. Al-zeyadi, "ARROW @ TU Dublin Intelligent SDN Traffic Classification Using Deep Learning : Deep-SDN," no. Iccci, 2020, doi: 10.21427/tbet-8c64.

[11] R. R. Sekar, A. M. Jenny, D. Sreshta, M. Vikas, D. B. N. Ajay, and M. Ganesh, "Prediction of Distributed Denial of Service Attacks in SDN using Machine Learning Techniques," *2023 3rd Int. Conf. Intell. Technol. CONIT 2023*, pp. 0–4, 2023, doi: 10.1109/CONIT59222.2023.10205887.

[12] A. Lakhan, M. A. Mohammed, O. I. Obaid, C. Chakraborty, K. H. Abdulkareem, and S. Kadry, "Efficient deep-reinforcement learning aware resource allocation in SDN-enabled fog paradigm," *Autom. Softw. Eng.*, vol. 29, no. 1, 2022, doi: 10.1007/s10515-021-00318-6.

[13] S. Prabakaran *et al.*, "Predicting Attack Pattern via Machine Learning by Exploiting Stateful Firewall as Virtual Network Function in an SDN Network," *Sensors*, vol. 22, no. 3, 2022, doi: 10.3390/s22030709.

[14] K. Sritharan, R. Elagumeeharan, S. Nakkeeran, A. Mohamed, B. Ganegoda, and K. Yapa, "Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation Testbed for SDN-Enabled IoT Devices," *2022 13th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2022*, 2022, doi: 10.1109/ICCCNT54827.2022.9984248.

[15] M. K. Awad, M. H. H. Ahmed, A. F. Almutairi, and I. Ahmad, *Machine Learning-Based Multipath Routing for Software Defined Networks*, vol. 29, no. 2. Springer US, 2021. doi: 10.1007/s10922-020-09583-4.

[16] M. Xiang, M. Chen, D. Wang, and Z. Luo, "Deep Reinforcement Learning- based load balancing strategy for multiple controllers in SDN," *e-Prime - Adv. Electr. Eng. Electron. Energy*, vol. 2, no. February, p. 100038, 2022, doi: 10.1016/j.prime.2022.100038.

[17] J. Malik, A. Akhunzada, I. Bibi, M. Imran, A. Musaddiq, and S. W. Kim, "Hybrid Deep Learning: An Efficient Reconnaissance and Surveillance Detection Mechanism in SDN," *IEEE Access*, vol. 8, pp. 134695–134706, 2020, doi: 10.1109/ACCESS.2020.3009849.

[18] D. Todorov, H. Valchanov, and V. Aleksieva, "Load Balancing model based on Machine Learning and Segment Routing in SDN," *2020 Int. Conf. Autom. Informatics, ICAI 2020 - Proc.*, 2020, doi: 10.1109/ICAI50593.2020.9311385.

[19] W. Sun, Z. Wang, and G. Zhang, "A QoS-guaranteed intelligent routing mechanism in software-defined networks," *Comput. Networks*, vol. 185, p. 107709, 2021, doi: 10.1016/j.comnet.2020.107709.

[20] W. xi Liu, J. Cai, Q. C. Chen, and Y. Wang, "DRL-R: Deep reinforcement learning approach for intelligent routing in software-defined data-center networks," *J. Netw. Comput. Appl.*, vol. 177, no. January, 2021, doi: 10.1016/j.jnca.2020.102865.

[21] A. Singh, G. S. Aujla, S. Garg, G. Kaddoum, and G. Singh, "Deep-Learning-Based SDN Model for Internet of Things: An Incremental Tensor Train Approach," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6302–6311, 2020, doi: 10.1109/JIOT.2019.2953537.