Volume: 5, Issue: 6
Page: 174-182
2021

International Journal of
Science and Business
Journal homepage: ijsab.com/ijsb

IJSAB International

Deep learning Utilization in SDN Networks: A Review

Shavan Askar, Kosrat Dlshad Ahmed, Shahab Wahhab Kareem

Abstract

The contexts of SDN or Software Defined Network deliver increased level of programmable and functionality within the network development, network configuration and development of the dynamic management in the software protocol. SDN concept also provides centralized management and development approach for the network selection, network control and data plans. In this paper, different deep learning models and technical processes for the SDN networks have been reviewed.

IJSB
Literature review
Accepted 29 May 2021
Published 19 August 2021
DOI: 10.5281/zenodo.5222205

Keywords:*Deep Leaning, Machine Learning, Cyber Security, Internet of Things, Privacy, Cyber Security.*

About Author (s)

Shavan Askar (Corresponding Author), Assistant Professor, CEO of Arcella Teleco, Erbil Polytechnic University, Erbil, Iraq. Email: shavan.askar@epu.edu.iq.
Kosrat Dlshad Ahmed, Information System Engineering, Erbil Polytechnic University, Erbil, Iraq. Email: kosrat.ahmed@epu.edu.iq.
Shahab Wahhab Kareem, Lecturer, Erbil Polytechnic University, Erbil, Iraq.

1. Introduction

The concept of Software Defined Networking or SDN is assessed as an adaptive, manageable, dynamic technology which serves different purposes in the context of the software management and evaluation (Yu et al. 2018). This architecture of SDN uses special management capability by which it separates the processing of data plane and control plane (Sendra et al. 2017). Considering this opportunity, the technology of software defined networking has opened different dimensions for effective participation and management capability for the technological processes (Lee et al. 2013). The amount of data that passes across networks and the variety of processing functions that are applied to it is both growing exponentially Effective network management is progressively depends on extracting information from this info. In our current model, the paradigm of Software Defined Networks (SDNs), new pathways are opened due to their knowledge collection capabilities and programmability (Sendra et al. 2017). The Openflow basic API is widely used in SDNs. Within the context of SDN, the control panel makes the decisions and effective performance for the packets processing for the network capability management (Askar, 2017; Fizi & Askar, 2016). It describes how to move information between the software and hardware flight control systems (Sendra et al. 2017). We examine what kinds of knowledge can be obtained from Openflow network data, as well as how it can be applied to network management tasks using this information (Lee et al. 2013). This research is an early move into an SDN usage of Machine Learning (ML) to track and manage business networks utilising the Openflow protocol. Several techniques have been developed to investigate the movement of traffic across a network. Usually, knowledge about the transport and directly examining the payload have been utilised in tandem. As a result, though, machine learning techniques are the preferred methodology in recent research, both methods have many issues (Sendra et al. 2017). Concepts and applications in this context. There are a variety of things that may happen, some examples are: Predicting network trends (e.g. traffic counts); Use of network resources (AEF, WAF, and DoS/DDoS detection It's possible that software-defined networks will simplify the use of apps like this in general network configurations (Sulaiman & Askar, 2015; Fares & Askar, 2016; Lange et al. 2015). They provide a software-defined separation between the data and forwarding plane (Sendra et al. 2017). There are built-in data collection methods as well as network behaviours that can be enforced without use of middleware. Computer efficiency has significantly increased in recent years as a result of hardware promotion (Li et al. 2019). As a result, deep learning has been commonly used to address a broad range of challenges, including image recognition and traffic analysis for different SDN networks. In the application of network intrusion detection and management processes, deep learning may allow classification and prediction through learning a vast volume of data for the development of the SDN system. As a result, the deep learning-enabled intrusion detection and prevention framework (DL-IDPS) will be proposed and implemented over SDN networks (Singh et al. 2021). Utilization of different deep learning methods and processes within the SDN networks, can be effectively utilized for managing the development and progression of the system models. The context of SDN expands to the practical utilization and management of the technological prospects for the assessment of the network capability and management considerations (Askar, 2016; Keti & Askar, 2015; Qadir & Askar, 2021; Singh et al. 2021). In this way, the management for the network capability can be considered to utilize improved utilization of the software and hardware integration.

2. Related Works

SDN (Software Defined Network) is described as a new networking system that separates available different forms of control and forwarding planes to support the detection and determination of the available components (Sendra et al. 2017). Packet forwarding machines (usually Openflow switches) in the forwarding plane deal with the actions of data packets depending on the forwarding tables received from the handler. The controllers own the ultimate vision of the network in the control plane and will therefore perform unified network control. The controller will monitor the actions of the switches by transmitting forwarding rules to them. In SDN systems, the components for single controller mode is impossible and impractical due to the vast number of different switches used in similar networks. The high volume of engaged traffic and the contexts of latency management and processing between the device arrangements and the switch make a single controller management system for the configuration difficult. SDN will greatly minimise network control and maintenance complexities while still encouraging network creativity, making it common in current network scenarios such as data centres. In addition, the implementation of the theoretically centralised control plane's physically dispersed architecture has been investigated. As a result, various and distributed controllers setup and developments have been suggested in the literature to increase and process the control plane's stability and scalability (Kaur et al. 2018). The basic challenge in the different aspects of distributed control plane is to solve and assess the controller positioning problem for SDN networks, which involves deciding the position of the controllers. Furthermore, after the controllers have been mounted, the problem of which direction each one is turning should be mapped should be solved (Li et al. 2019). As explained in the tutorial, the transition to controller mapping explains the relationship between the switch controller and the network (Lange et al. 2015). This has been well discussed in the literature with the emphasis on controller count and placement, so there is no need to repeat it here. Most controllers seek to solve the issue by using resources more carefully, increasing reaction speed, or taking into account several perspectives. current research works, on the other hand, tackle the switch controller mapping issue using real-time network context details such as controller traffic load, operating state, and resource usage. The topology of the networks, on the other hand, can be complex and shift over time. For example, a controller malfunction can cause the controller to exit the device. Given this, it's preferable to map this freshly joined transition to a controller with a lower failure rate (Rasool et al. 2019). As a result, the mapping decision can be influenced by time-varying network dynamics (Lee et al. 2013). This complicates the switch controller mapping issue since the switch controller mapping optimization judgement must take into account not just the current device state but also the network environment's time-varying characteristics (Singh et al. 2021). A few research projects have been created to respond to the changing network traffic scenario. As a result, the mapping approach can be influenced by time-varying network dynamics. If a switch is connected to a controller that could malfunction in the future, for example, there may be an extra expense to migrate the switch (Lee et al. 2020). However, the previously described research work focuses on long-term time-average efficiency enhancement for lowering device operating costs while only taking traffic fluctuations into account (Lee et al. 2020). The controller and switch dynamics, such as controller and switch entering and quitting due to network topology dynamics, were not taken into account. Internet of Systems has been considered to be opened the way for the transformation of the traditional industrial market to Industry 4.0, an automated and interactive revolution. A network of linked machines (sensors or actuators) is developed under this umbrella, with the data provided by these machines being gathered and evaluated for better decision making for the software based systems. The machines and systems used in this self-contained Industrial setup for the deep learning provision can communicate with one another, relay data, and collaborate to achieve broader industrial goals. This massive amount and conceptualization of data sources (volume), which is modified and analyzed frequently in relation with the systematic analysis (velocity) and produced in a variety of formats that are used in the system (variety), must be computationally formulated and analyzed in order to uncover secret trends and correlations (internal/external). The data's latent dynamics aid in bettering decision-making and corporate practices, resulting in improved efficiency, cost-effectiveness, and accuracy (Lee et al. 2020). The whole method of processing, sharing, and reviewing big data erodes the underlying concepts for the network infrastructure processes and enabling architectures' functionality significantly (Lee et al. 2020). This will result in greater inefficiencies within the system and delayed operations/workflows, which can have a negative effect on total industrial outputs. This necessitates the use of adaptive network technologies that can maintain consistency even while under a lot of stress (Xue et al. 2018). The close linking or binding of different aspects of control and data forwarding activities in traditional network design does not meet these criteria or specifications (Xue et al. 2018). Traditional TCP/IP design, for example, may accommodate end-to-end communications yet isn't modular enough to federate the pervasive implementation or disbanding of forms of remote network enabling machines at geographically scattered industrial locations (Xue et al. 2018). This challenge highlights the need for a scalable and agile network design in which data forwarding processes are isolated from control capability. One of the suitable solutions is Software Defined Networking (SDN), and systematic approaches which provides logically unified control functionality through decoupled data and control planes (Lee et al. 2020). Most industrial networks cope with a combination of applications, time-sensitive and legacy applications that need various network mechanisms, increasing the network architecture's complexity (Askar et al., 2011; Al Majeed et al, 2014; Singh et al. 2021). In such cases, though, SDN will continue to improve the network by including a versatile and multi-tenant design. When it lands in the digital room, the race for continuous access for distributing high-fidelity data from the central level to all the components in an Industrial device contributes to some protection complications (Lee et al. 2020). SDN, on the other hand, makes core business activities easier by offering a dependable and stable connectivity system (Singh et al. 2021). Furthermore, in the above-mentioned mixed-mode application case, the need for constant and sustained communication results in low visibility, reducing the capacity to shield and protect either device. Any SDN vendors sell layer 3 encryption technology, although others contend that it is prohibitively expensive and impossible to implement. SDN helps here in it has global exposure that enables businesses to monitor and maintain the overall network protocol presence, and dependable network management (Lee et al. 2020). All in one place means SDN has several challenges, for example, it is vulnerable to single points of failure (Lee et al. 2020). An opponent will soon take over the controller, clogging the entire network and inserting bogus legislation, are still a problem for governments, said Bogdanoff. Authentication can also be integrated into an SDN strategy to guarantee the accessibility, security, and privacy of information. a modern safety mechanism called Next-Generation SDN decouples protection from network traffic and firewall control planes. A framework for planning, installing, and monitoring, for network controls (such as firewalls) has been built into SEC (Lee et al. 2020).

While layer 3 encryption is safe, certain businesses use mutual orchestration, through which the infrastructure is managed by a third party (Singh et al. 2021). Furthermore, SDN architecture's simplicity allows for the addition of additional infrastructure from a variety of suppliers or providers. However, the challenge is how to maintain the new connection's stability. Furthermore, deploying the widely used application level encryption not only adds overhead and limits bandwidth, but it also has an effect on latency and throughput (Singh et al. 2021). If data source systems are to be investigated, security solutions must be disabled, making the enterprise vulnerable to attackers. The separation of resources and protection from management and maintenance in SDN architecture will protect sensitive business assets (Singh et al. 2020). Via its distributed infrastructure, Blockchain technology may be used to have the desired disaggregation throughout this path (Wu et al. 2020; Husain & Askar, 2021; Samann et al, 2021). It therefore eliminates dependency on a single point of vulnerability and follows a protection architecture that is independent of the underlying network infrastructure (Singh et al. 2020). Furthermore, the permissioned blockchain will implement the advantages of centralized management for improved control and uniformity (Abdulkahleq & Askar, 2021; Khalid & Askar, 2021; Tapia et al. 2013). The blockchain not only secures the SDN infrastructure, but it also aids in the tracking of network insights and results (Singh et al. 2020). Furthermore, it guarantees that data points, incoming traffic, and external attacks are all investigated simultaneously without the monitoring protocols being turned off (Tapia et al. 2013). The data source, the owner, the final destination, future paths, protection provisions, and security enabling authority may all be tracked using blockchain (Singh et al. 2020) It is unconcerned with network infrastructure, preferring to ensure disaggregated and agnostic security orchestration.

3. Methodology

This research will follow positivist philosophical approach in order to facilitate effective determination of different research outcomes. In this way, the effective management and determination of the outcomes of this research can be effectively determined (Tapia et al. 2013). To conduct this systematic review, definite resources and strategic components have been adopted in this report. Allocation and management of time and resources have been aligned so that the author can evaluate the findings in justified approach. In this way, selection of the approaches has been conducted effectively.

The search criteria for this research, includes conduction of the searching of the journals by using definite keywords such as deep learning, SDN, Software Defined Networks, Resource attribution, etc. Only reliable and valid data sources have been selected in the search process. Articles that are published between 2015 and 2021, have been included in the comparative analysis of the journals. In this process, definite selection of the data base and resources have been included in the search process. Based on the availed resources and journals, the comparative analysis has been conducted in this assessment.

Ethical considerations have been maintained effectively in this research. Data has been collected only from the reliable and valid sources. In this way, the collection and analysis of the data have been conducted effectively. To conduct the overall research, selection of appropriate resources and capabilities have been ensured.

4. Analysis and Findings

Table 1. Comparing Literature

Authors	Findings
Qin et al. (2019)	Authors analyzed the rapid progression and development of the recent technological capability and demonstration of the keen learning on the SDN facilities (Lee et al. 2020). The authors outlined that apart from the features of traditional networks, the concept of SDN is programmable in which the operators can modify the setup and development of the SDN networks. Within the development phase of the SDN facilities, the security and programmability features were considered as highly important for the development of the Convolutional Neural Network. (Qiao et al. 2020) CNN and RNN or Recurrent Neural Network are the basis for different aspects of the network processing system. Development of the deep learning methods for effective resource management.
Singh et al. (2021)	Machine learning is commonly used to overcome anomaly-based identification approaches. Signature and anomaly detection are often used in intrusion detection. Some recognized attack forms can be detected with high precision using signature-based methods (Lee et al. 2020). The unknown threat, on the other hand, is undetectable. After designing the characteristics of the network flows, a machine learning algorithm is used to detect new attack network flows. The architecture of network flow elements, on the other hand, is a difficult challenge. Similar assault styles can be influenced by various characteristics. It has the benefit of detecting new forms of attacks as well as understanding recognized types of attacks. Furthermore, the detection system focused on machine learning has a poor detection score.
Fan et al. (2020)	The two different ways spectrum-allocation schemes are called 'underlay' and 'overlay' (Singh et al. 2020). The V2X underlay and cellular devices have the same frequency levels, causing equal interruption. While C-V2X users would need shared cellular bandwidth for data transmission, the offloading of traffic is more complicated for V2X networks. Wired and wireless users have separate frequencies in the overlaid on the V2 device, enabling two communications to take place in the same frequency range. Increasing the number of V2 devices has the greater impact on Quality of Service (QoS) since additional spectrum is allocated to these devices (Singh et al. 2020). Because of this, V2X and cellular interactions must be heavily rely on each other, resulting in more complex and effective resource allocation procedures. Deep learning implications for assessing the implications for the SDN cellular V2X can be implemented. In this paper, authors have different aspects for the traffic load balance and improving the contexts for the network congestion.
Lee et al. (2020)	The authors described that SDN networks dynamically divides a network in several data and control planes. In this centralized management procedures, effective management of the deep learning association and differentiation of the network prospects have been conducted.
Singh et al (2020)	The authors have considered different aspects of IoT or internet of things as the revolutionary model for technological accumulation of the faster delivery and management of the data correspondence (Singh et al. 2020). Data attributes to conduct the definite approaches for the technological processes can be asserted for the determination of the multidimensional data and information.
Wu et al. (2020)	It is important to understand both the network topology and flow characteristics in order to get the optimal solution. Dynamic data driven design using Deep Q-Networks (DQN) (D4CPP). Furthermore, D4CP integrates past network details to controller information into deployment and incorporates real-time switch-mapping strategies. Permissive D4P, the datacenter respects the fluctuation, data latency, and load balancing, and can get an optimum performance balance (Qiao et al. 2020). Dealing with the enormous amount of data available in today's world and dramatic changes in the world's information will get positive results by using deep reinforcement learning (DRL) and learning by trial and error. Controller positioning is a major issue of Software Defined Networking (SDN), and has been proposed as a way to gain more flexible network access and management. Extensive simulations demonstrate that D4CPP outperforms standard schemes in SDN systems with complex flow fluctuations (Qiao et al. 2020).
Rasool et al. (2019)	With just network traffic authentication, mitigating LFA on the control channel remains a problem in the network protection model. The concept of a centralised controller becomes a bottleneck since it exposes a wide range of weaknesses to different forms of attacks. In this article, we show how the SDN system architecture is vulnerable to LFA and how the attack technique varies from conventional malicious activities, which mainly include attacking the ties directly (Mao et al. 2018). The connection flooding attack was among the most dangerous, stealthy, and simple attacks against networked systems (LFA). In LFA, the intruder uses bots to deliver low-rate legal traffic on the control channel invisibly, resulting in the sdn controller being disconnected from the transport layer.
Alonso et al. (2020)	As in this sense, smart systems such as deep learning techniques are supposed to refine virtual data flows in the virtual networks, deep reinforcement learning approaches are expected to be helpful. Many organisations are already turning to software-defined networking and network modules in order to save costs. the internet of things and the countless sensors and thousands of connected to the cloud (Mnih et al. 2015). More and more importantly, edge computing has emerged as a way of lowering the costs and complications associated with extracting, accessing, processing, and storing IoT ecosystem data With all of these vast amounts of data being gathered and processed, organisations have a better understanding of just what they are looking for (Tapia et al. 2013). Through analysing the data at the network's edge, we are able to have quicker response times, including in the face of connection failures at the IoT layer (Mao et al. 2018; Ahmed & Askar, 2021; Mohammed & Askar, 2021; Ali & Askar, 2021; Hamad & Askar, 2021).

5. Discussion and Analysis

From the discussion of the papers, this is obvious that different aspects of deep learning attributes have greater implications on the SDN networks (Mao et al. 2018). The size of data center networks is constantly evolving due to the exponential development of cloud storage, big data, and other technology. Owing to network management and integration challenges, conventional networks are unable to address the needs of existing communication networks.

The advent of SDN points to a solution to the issue described above. It's an innovative transmit antennas in which the forwarding device's control plane and data plane are separated (Mao et al. 2018). Routing solutions focusing on a global vision of the network can be deployed easily and flexibly with the help of SDN. They are challenging to obtain optimum solutions in the face of the changing network world. The rise of AI has given us a modern way to solve the routing dilemma. From the evaluation of the papers, this is obvious that organisations need to adopt different forms of data evaluation and strategic approaches to render effective outcome for the assessment. Data centers would be able to make better choices with the use of SDN Routing has long been an area of deep study of data centre networks. With the proliferation of data centres and computing centres, there is a need for networks to be separated into elephant-sized flows and mouse-sized flows. Elephants flow a lot of data and last a long time Source: As a result of today's network-oriented traffic patterns, study is mainly conducted on SDN-based approaches in data centre networks (Mnih et al. 2015). Manual application of each of these routing schemes is needed.

6. Conclusion

In modern data centers, the concept of SDN is growing at increasing pace which has been impacting on the actual scenario of the business world. In order to complement the real world aspects for the complex formation and development of the data centers and management capability, separate data, application and control need to be adjusted for the management of the technological processing. In this research, the variance and application of different deep learning models for the SDN networks have been defined to propose effective model for practical utilization.

References

Abdulkhaleq, I. S., Askar, S. (2021). Evaluating the Impact of Network Latency on the Safety of Blockchain Transactions. International Journal of Science and Business, 5(3), 71-82.

Ahmed, K. D., Askar, S. (2021). Deep Learning Models for Cyber Security in IoT Networks: A Review. International Journal of Science and Business, 5(3), 61-70

Al Majeed, S., Askar, S., Fleury, M. (2014). H.265 Codec over 4G Networks for Telemedicine System Application. UKSim-AMSS 16th International Conference on Computer Modelling and Simulation (UK), Cambridge (pp. 292-297), doi: 10.1109/UKSim.2014.59.

Ali, K., Askar, S. (2021). Security Issues and Vulnerabilities of IoT Devices. International Journal of Science and Business, 5(3), 101-115.

Alonso, I. Sittón-Candanedo, R. Casado-Vara, J. Prieto and J. M. Corchado, (2020). "Deep Reinforcement Learning for the management of Software-Defined Networks in Smart Farming," 2020 International Conference on Omni-layer Intelligent Systems (COINS), Barcelona, Spain, 2020, pp. 1-6, doi: 10.1109/COINS49042.2020.9191634.

Askar S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Evaluation of Classified Cloning Scheme with self-similar traffic. 3rd Computer Science and Electronic Engineering Conference (CEEC), Colchester, 2011, pp. 23-28, doi: 10.1109/CEEC.2011.5995819.

Askar, S. (2016). Adaptive Load Balancing Scheme For Data Center Networks Using Software Defined Network. Journal of University of Zakho, Vol. 4(A), No.2, Pp 275-286,

Askar, S. (2017). SDN-Based Load Balancing Scheme for Fat-Tree Data Center Networks. Al-Nahrain Journal for Engineering Sciences (NJES), Vol.20, No.5, pp.1047-1056

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Service differentiation for video applications over OBS networks. 16th European Conference on Networks and Optical Communications, Newcastle-Upon-Tyne, pp. 200-203.

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). A novel ingress node design for video streaming over optical burst switching networks. Optics Express, Vol. 19 (26), pp. 191-194

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Adaptive Classified Cloning and Aggregation Technique for Delay and Loss sensitive Applications in OBS Networks. in Optical Fiber Communication Conference/National Fiber Optic Engineers Conference 2011, OSA Technical Digest (CD) (Optical Society of America, 2011), paper OThR4.

Bangzhou Liu, Binqiang Wang, and Xiaoqiang Xi, (2016). “Heuristics for sdncontroller deployment using community detection algorithm,” in 20167th IEEE International Conference on Software Engineering and Service Science (ICSESS), pp. 253–258, Aug 2016.

Bontemps, V. L. Cao, J. McDermott, and N. A. Le-Khac, (2016). “Collective anomaly detection based on long short-term memory recurrent neural networks,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2016.

Chaudhary, G. S. Aujla, N. Kumar, and J. J. P. C. Rodrigues, (2018). “Optimized big data management across multi-cloud data centers: Software-defined network-based analysis,” IEEE Communications Magazine, vol. 56, no. 2, pp. 118–126, Feb 2018.

Dixit, F. Hao, S. Mukherjee, T. V. Lakshman, and R. Kompella, (2014). ‘‘ElastiCon: An elastic distributed sdn controller,’’ in Proc. 10th ACM/IEEE Symp. Archit. Netw. Commun. Syst. (ANCS), Oct. 2014, pp. 17–27.

Fan, Z. He, Y. Wu, J. He, Y. Chen and L. Jiang, (2020). "Deep Learning Empowered Traffic Offloading in Intelligent Software Defined Cellular V2X Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 11, pp. 13328-13340, Nov. 2020, doi: 10.1109/TVT.2020.3023194.

Fares, N., Askar, S. (2016). A Novel Semi-Symmetric Encryption Algorithm for Internet Applications. Journal of University of Duhok, Vol. 19, No. 1, pp. 1-9

Fizi, F., & Askar, S. (2016). A novel load balancing algorithm for software defined network based datacenters,International Conference on Broadband Communications for Next Generation Networks and Multimedia Applications (CoBCom), Graz, 2016, pp. 1-6, doi: 10.1109/COBCOM.2016.7593506.

Hamad, Z., Askar, S. (2021). Machine Learning Powered IoT for Smart Applications. *International Journal of Science and Business, 5*(3), 92-100.

Heller, R. Sherwood, and N. McKeown, (2012). "The controller placement problem," in Proceedings of the first workshop on Hot topics in software defined networks. ACM, 2012, pp. 7-12.

Husain, B. H., Askar, S. (2021). Survey on Edge Computing Security. International Journal of Science and Business, 5(3), 52-60.

Jimenez, C. Cervello-Pastor, and A. J. Garcia, (2014). ‘‘On the controller placement for designing a distributed SDN control layer,’’ in Proc. IFIP Netw. Conf., Jun. 2014, pp. 1–9.

Kaur, S. Garg, G. S. Aujla, N. Kumar, J. J. P. C. Rodrigues, and M. Guizani, (2018). “Edge computing in the industrial internet of things environment: Software-defined-networks-based edge-cloud interplay,” IEEE Communications Magazine, vol. 56, no. 2, pp. 44–51, Feb 2018.

Keti, F., Askar, S. (2015). Emulation of Software Defined Networks Using Mininet in Different Simulation Environments. 6th International Conference on Intelligent Systems, Modelling and Simulation, Kuala Lumpur, 2015, pp. 205-210, doi: 10.1109/ISMS.2015.46.

Khalid, Z., Askar, S. (2021). Resistant Blockchain Cryptography to Quantum Computing Attacks. International Journal of Science and Business, 5(3), 116-125.

Lange, S. Gebert, T. Zinner, P. Tran-Gia, D. Hock, M. Jarschel, and M. Hoffmann, (2015). ‘‘Heuristic approaches to the controller placement problem in large scale SDN networks,’’ IEEE Trans. Netw. Service Manage., vol. 12, no. 1, pp. 4–17, Mar. 2015.

Lee, L. Chang and C. Syu, (2020). "Deep Learning Enabled Intrusion Detection and Prevention System over SDN Networks," 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Dublin, Ireland, 2020, pp. 1-6, doi: 10.1109/ICCWorkshops49005.2020.9145085.

Lee, M. S. Kang, and V. D. Gligor, (2013). ‘‘CoDef: Collaborative defense against large-scale link-flooding attacks,’’ in Proc. 9th ACM Conf. Emerg. Netw. Exp. Technol., 2013, pp. 417–428

Li, X. Xu, H. Yao, J. Wang, C. Jiang, and S. Guo, “Multi-controller resource management for software-defined wireless networks,” IEEE Communications Letters, vol. 23, pp. 506–509, March 2019.

Mao, F. Tang, Z. M. Fadlullah, N. Kato, O. Akashi, T. Inoue, and K. Mizutani, (2018). ‘‘A novel non-supervised Deep-Learning-Based network traffic control method for software defined wireless networks,’’ IEEE Wireless Commun., vol. 25, no. 4, pp. 74–81, Aug. 2018.

Mnih, K. Kavukcuoglu, D. Silver, A. Rusu, J. Veness, M. Bellemare, A. Graves, M. Riedmiller, A. Fidjeland, G. Ostrovski, S. Petersen, C. Beattie, A. Sadik, I. Antonoglou, H. King, D. Kumaran, D. Wierstra, S. Legg, and D. Hassabis, (2015). “Human-level control through deep reinforcement learning,” Nature, vol. 518, pp. 529–33, 02 2015.

Mohammed, C. M., Askar, S. (2021). Machine Learning for IoT HealthCare Applications: A Review. International Journal of Science and Business, 5(3), 42-51.

Qadir, G. A., Askar, S. (2021). Software Defined Network Based VANET. International Journal of Science and Business, 5(3), 83-91.

Qiao, S. Leng, S. Maharjan, Y. Zhang, and N. Ansari, (2020). “Deep reinforcement learning for cooperative content caching in vehicular edge computing and networks,” IEEE Internet of Things Journal, vol. 7, pp. 247–257, Jan 2020

Qin, J. Wei and W. Yang, (2019) "Deep Learning Based Anomaly Detection Scheme in Software-Defined Networking," 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 2019, pp. 1-4, doi: 10.23919/APNOMS.2019.8892873.

Rasool, Raihan & Ashraf, Usman & Ahmed, Khandakar & Wang, Hua & Rafiq, Wajid & Anwar, Zahid. (2019). CyberPulse: A Machine Learning based Link Flooding Attack Mitigation System for Software Defined Networks. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2904236.

Samann, Fady E. F., Zeebaree, S. RM, Askar, S. IoT Provisioning QoS based on Cloud and Fog Computing, Journal of Applied Science and Technology Trends, Vol. 2, No. 1, pp. 29-40.

Sendra, A. Rego, J. Lloret, J. M. Jimenez, and O. Romero, (2017). ''Including artificial intelligence in a routing protocol using software defined networks,'' in Proc. IEEE Int. Conf. Commun. Workshops, May 2017, pp. 670–674.

Singh, G. S. Aujla, A. Singh, N. Kumar and S. Garg, (2021). "Deep-Learning-Based Blockchain Framework for Secure Software-Defined Industrial Networks," in IEEE Transactions on Industrial Informatics, vol. 17, no. 1, pp. 606-616, Jan. 2021, doi: 10.1109/TII.2020.2968946.

Singh, G. S. Aujla, S. Garg, G. Kaddoum and G. Singh, (2020). "Deep-Learning-Based SDN Model for Internet of Things: An Incremental Tensor Train Approach," in IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6302-6311, July 2020, doi: 10.1109/JIOT.2019.2953537.

Sulaiman, S., Askar, S. (2015). Invetigation of the Impact of DDoS Attack on Network Efficiency of the University of Zakho. Journal University of Zakho, Vol. 3(A) , No.2, Pp 275-280.

Tapia, R. S. Alonso, O. Garc ´ ´ıa, F. de la Prieta, and B. Perez- ´ Lancho, (2013). "Cloud-io: cloud computing platform for the fast deployment of services over wireless sensor networks," in 7th International Conference on Knowledge Management in Organizations: Service and Cloud Computing. Springer, 2013, pp. 493–504.

Wu, S. Zhou, Y. Wei and S. Leng, (2020). "Deep Reinforcement Learning for Controller Placement in Software Defined Network," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 2020, pp. 1254-1259, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162977.

Xue, X. Ma, X. Luo, E. W. W. Chan, T. T. Miu, and G. Gu, (2018). ''LinkScope: -Toward detecting target link flooding attacks,'' IEEE Trans. Inf. Forensics Security, vol. 13, no. 10, pp. 2423–2438, Oct. 2018.

Yu, J. Lan, Z. Guo, and Y. Hu, (2018). ''DROM: Optimizing the routing in software-defined networks with deep reinforcement learning,'' IEEE Access, vol. 6, pp. 64533–64539, 2018.

Cite this article:

Shavan Askar, Kosrat Dlshad Ahmed, Shahab Wahhab Kareem (2021). Deep learning Utilization in SDN Networks: A Review. *International Journal of Science and Business, 5*(6), 174-182. doi: https://doi.org/10.5281/zenodo.5222205

Retrieved from http://ijsab.com/wp-content/uploads/754.pdf

Published by

IJSAB International