Indonesian Journal of Computer Science
ISSN 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam No. 1, Padang, Indonesia
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

Challenges and Outcomes of Combining Machine Learning with Software-Defined Networking for Network Security and Management Purpose: A Review

Nura Jamal Bilal [1*)], Shavan Kamal Askar[2], Karwan M. Muheden, Mariwan Mohammed
[1]noura.bilal@epu.edu.iq , [2]shavan.askar@epu.edu.iq
Information System Engineering Department, Technical Engineering College, Erbil Polytechnic University, Erbil

Article Information

Submitted : 20 Mar 2024
Reviewed: 25 Mar 2024
Accepted : 8 Apr 2024

Keywords

Software-Defined Networking (SDN), Machine Learning (ML) Anomaly Detection, Security, Deep Learning

Abstract

Current research in data dissemination in Vehicular Ad Hoc Networks (VANETs) has examined different approaches and frameworks to enhance the effectiveness and dependability of information sharing between vehicles on the road. The integration of Machine Learning (ML) with Software-Defined Networking (SDN) has fundamentally transformed the field of network administration and security. This paper specifically addresses the challenges faced by traditional network architectures in effectively handling the increasing amount of data and complex applications. Software-Defined Networking (SDN), a cutting-edge framework, separates the control of network operations from the actual forwarding of data, offering a versatile and cost-effective solution. The combination of Software-Defined Networking (SDN) and Machine Learning (ML) allows for the extraction of valuable information from network data, leading to enhanced network management and the facilitation of predictive analytics. The aim of this study is to examine the feasibility and challenges of incorporating machine learning into software-defined networking (SDN), focusing particularly on practical applications. Integrating Machine Learning (ML) into Software-Defined Networking (SDN) presents challenges, including the requirement for robust algorithms to detect patterns and ensure security. It is crucial to carry out the tasks of developing and implementing machine learning models for real-time predictions and ensuring the robustness of the system. Research is essential to strike a balance between the transformative abilities of ML-SDN and the practical network environments. This helps to improve the resilience, security, and adaptability of network infrastructures in the digital age.

Attribution-ShareAlike 4.0 International License

A. Introduction

The integration of Software-Defined Networking (SDN) and Machine Learning (ML) has brought about a substantial transformation in the field of network administration and security in recent years. Conventional network structures have faced difficulties in adjusting to the growing amounts of data streams and the intricacy of applications. Software-Defined Networking (SDN), as an innovative framework, divides the control and forwarding functionalities of a network, providing a flexible, economical, and adaptable solution. SDN is well-suited for the dynamic nature of modern applications because network control can be directly programmed as a result of this division. The integration of Software-Defined Networking (SDN) and Machine Learning (ML) enables the retrieval of valuable information from network data, resulting in improved network administration and anticipatory data analysis. Several research studies [1-4] demonstrate the exploration of the intersection between machine learning and software-defined networking (SDN), examining various aspects of this field. Software-defined networking (SDN) is a network architecture that divides network control and data forwarding. By incorporating Artificial Intelligence (AI) and Machine Learning (ML) into Software-Defined Networking (SDN), its capabilities are improved, allowing it to better adjust to changing network conditions. The investigation of machine learning in software-defined networking (SDN) is motivated by the desire for improved network management solutions that provide increased flexibility, safety, and effectiveness. Machine learning is highlighted in the literature for its capacity to tackle important challenges in software-defined networking (SDN), such as intelligent routing, intrusion detection, traffic control, and optimization. There is an urgent need for new methods to improve the ability of networks to withstand and adapt to cyber threats and the constantly changing network environments. The capacity of machine learning to detect patterns in data and generate perceptive forecasts has the potential to revolutionize SDN, transforming it into a network architecture that optimizes and safeguards itself. The references analyzing reinforcement learning [5-8], anomaly detection [9-12], and security applications [13-15] demonstrate that the motivation is strengthened by the established achievements of machine learning applications in networking contexts. Our research's main goal is to examine the possibilities and difficulties of incorporating machine learning into SDN, with an emphasis on useful applications. Through a thorough reading list that includes papers on routing optimization [16-18], intrusion detection [19-21], among others, we want to uncover new approaches and frameworks that further the development of ML-driven SDN solutions. Our study is unique in that it synthesizes results from other studies to suggest novel ways to tackle particular problems in SDN, which improves its overall performance, security, and adaptability. In order to establish the groundwork for the creation of intelligent, self-learning networks that can successfully navigate the intricacies of the contemporary digital landscape, we seek to offer insightful analysis of ML algorithms' efficacy within the framework of SDN. This innovative architecture enables the direct programmability of network control and abstracts the underlying infrastructure for network services and applications by separating network control and forwarding functions [22-23]. Figure 1 showcases the modular and adaptable characteristics of the SDN architecture, while also highlighting its intricate details. The OpenFlow protocol [24-25] is widely respected and serves as the foundation for numerous SDN implementations, enabling the construction of SDN systems. This protocol facilitates the communication between the hardware of the data plane and the software-operating controller plane, thereby simplifying the management and operation of the SDN environments.

B. Introduction

II. ROLE OF ML IN SDN

A. Traffic Prediction

Artificial intelligence (AI) and machine learning (ML) algorithms utilize historical data to forecast patterns in network traffic. This facilitates the allocation of resources and the administration of traffic more efficiently. This study investigates the application of deep learning (DL) and machine learning (ML) methods to classify and predict traffic in Software Defined Networking (SDN). The authors, who work at the University of Ottawa in Canada's DISCOVER Lab, concentrate on employing sophisticated computational techniques to maximize the potential of SDN. The objective of the research is to tackle traffic control challenges in SDN through the utilization of machine learning (ML) and deep learning (DL) methodologies. The study aims to explore the creation and use of algorithms to categorize network traffic and anticipate its trends, to improve the effectiveness and adaptability of SDN configurations [26]. The study [27-28] investigates different machine-learning methodologies and specifically focuses on the categorization of traffic within Software Defined Networks (SDNs). The study investigates the strategies and results of employing machine learning algorithms to accurately categorize network traffic in the context of Software-Defined Networks (SDNs), as illustrated in Figure 2. The objective of the research is to improve the routing paths and decrease the delay in Software Defined Networks (SDN) by utilizing deep learning algorithms for predicting traffic. The article likely explores the methods and results of using deep learning to implement predictive traffic analysis, to improve network performance [29]. The objective of the study is to improve the ability to differentiate network traffic in software-defined networks (SDNs) by employing ensemble and deep autoencoder techniques. The study aims to examine the methods and results of using these approaches to enhance the effectiveness and precision of network traffic discrimination in SDN systems [30-31].

B. 2.2. Anomaly Detection

Security threats and anomalous network behavior are detected using AI and ML. They can identify abnormalities by gaining knowledge from typical network activity. The effect of a machine learning strategy on Software-Defined Networking (SDN) anomaly detection via flow-based analysis is investigated in this research. Figure 3 shows the network flow, and this study intends to examine how the SDN environment can be enhanced to detect anomalies in this flow using machine learning techniques [32]. The study introduces Deep IDS, a deep learning method for detecting Software Defined Networking (SDN) intrusions. Research in this area usually looks at how and what happens when deep learning algorithms are used to make intrusion detection systems work better within the framework of SDNs [33]. Software-defined networking (SDN) anomaly detection is presented in the article [34] using a deep learning approach. An anomaly detection system built on top of SDNs and powered by deep learning will probably be the main emphasis of the research. This paper presents an Intrusion Detection System (IDS) that uses machine learning techniques and is designed for Software Defined Networks (SDNs). This paper mainly focuses on creating and assessing an intrusion detection system for Software-Defined Networks (SDNs) that makes use of machine learning techniques. Research in this area is likely to delve deeply into machine learning and how it improves software-defined network security.

C. Network Optimization

Through the utilization of data-driven real-time adaptations to routing, quality-of-service policies, and resource allocation, machine learning and artificial intelligence improve network performance. seeks to maximize SDN routing efficiency through the application of deep reinforcement learning. The authors analyze the theoretical foundations and design of the SDN paradigm to enhance routing methods [36]. This research aims to enhance the efficiency and responsiveness of network management in software-defined networks (SDNs) by exploring the potential of utilizing deep reinforcement learning. The objective is to discover a new approach that can improve the responsiveness and flexibility of SDN routing. The primary objective of the research [37] is to develop and implement an intelligent SDN framework that utilizes deep extreme learning machines to enhance routing decisions. An analysis of the fundamental principles of cognitive routing is attainable, with an emphasis on enhancing SDN decision-making by utilizing deep learning methods. Additional details regarding the DELM approach, including its methodology and potential benefits for enhancing cognitive routing, are anticipated to be disclosed shortly. This information will contribute to the ongoing discourse surrounding intelligent SDN frameworks [37]. Refer to [38] for additional information regarding the utilization of Deep Q-Network (DQN) and traffic prediction in SDNs to enhance routing efficiency. This research aims to investigate the potential of traffic prediction methods and DQN, a reinforcement learning approach, in improving the effectiveness of SDN routing decisions. The authors should consider exploring the theoretical foundations of DQN and its potential application in enhancing routing techniques through integration with traffic prediction algorithms. Readers are expected to comprehend the proposed approach, potential benefits, and overall influence of combining DQN and traffic prediction for SDN routing optimization.

C. Introduction

III. IMPLEMENTATIONS OF MACHINE LEARNING IN SOFTWARE-DEFINED NETWORKING (SDN)

A. Improved Network Traffic Engineering and Quality of Service (QoS) Management

Utilization of Machine Learning and Artificial Intelligence is progressively being employed to enhance traffic routing and oversee network quality in SDN environments. This entails utilizing AI-powered methods to dynamically modify network attributes according to the transmitted content, thereby improving resource allocation and productivity. In addition, machine learning models enhance user experience by prioritizing network traffic based on service requirements, incorporating artificial intelligence to effectively manage data flow in network environments such as the Internet of Things (IoT) and 6G. The user's text consists of the references [37,38].

B. Enhanced Security Solutions

AI-powered anomaly detection systems play a critical role in enhancing network security in Software-Defined Networking (SDN). The OpenStackDP framework utilizes SDN concepts to enhance network security mechanisms, incorporating machine learning for intrusion detection and threat mitigation as shown in Figure 4 [39,40]. Deep Learning techniques, incorporated in DeepIDS technology, scrutinize network activity to detect intrusions, thereby greatly improving the accuracy and efficiency of security protocols in SDN environments [41].

C. Resource Allocation in Real Time

Advanced machine learning algorithms are currently employed to dynamically allocate resources in 5G network slicing and fog computing, effectively tackling the difficulties associated with managing resources in fluctuating network conditions. To enhance efficiency in resource-constrained environments, it is recommended to employ techniques such as integer linear programming and Collaborative Machine Learning models, which can optimize resource utilization [42]. This approach is essential for scenarios like disaster management and the optimal functioning of IoT systems as shown in Figure 5 and Figure 6 [43,44].

D. Introduction

IV. BENEFITS OF AI AND ML IN SDN

A. Improved Efficiency

Artificial intelligence (AI) and machine learning (ML) streamline network management processes by automating tasks, thereby minimizing the requirement for manual intervention. Investigates the utilization of machine learning methods to optimize the detection of collision flow in 5G networks that utilize Software-Defined Networking (SDN)[31]. The convergence of machine learning, 5G technology, and SDN represents the shift in network communication. Applying machine learning methods to analyze collision flow detection provides valuable insights into possible technological synergies. This study emphasizes on implementing effective tactics to enhance the efficacy of network operations in light of the progress in communication technology[49].

B. Real-Time Adaptability

Integrating Software-Defined Networking (SDN) with Artificial Intelligence (AI) and Machine Learning (ML) allows for a quick and efficient response to changes in the network. The traffic management in Internet of Things (IoT) backbone networks is effectively handled by combining Graph Neural Network (GNN) and Multi-Armed Bandit (MAB) algorithms with Software-Defined Networking (SDN) orchestration, using an innovative approach. The objective of this integration is to establish a responsive traffic management system capable of swiftly adjusting to the changing demands of IoT environments [49]. The ability to adapt in real-time is crucial in Internet of Things (IoT) scenarios due to the frequent and abrupt changes in traffic patterns and network demands. This study highlights the significance of integrating sophisticated machine learning methodologies with software-defined networking (SDN) orchestration, particularly the GRASP and MAB algorithms. This integration enables the development of a traffic management system that can rapidly adjust to the dynamic characteristics of IoT backbone networks. The topic of [51] in software-defined networking (SDN) revolves around the application of machine learning (ML) to swiftly identify and mitigate distributed denial-of-service (DDoS) attacks. The authors propose using data collected from SDN environments to train a machine-learning model capable of extracting relevant features for real-time monitoring. The model detects anomalies and potential Distributed Denial of Service (DDoS) attacks in network traffic to assist in implementing automated mitigation strategies.

E. Introduction

V. CHALLENGES AND CONCERNS

Advancements in Network Security Addressing Conventional Challenges with Innovations

Discussion of new developments and ongoing issues in network security, with a focus on privacy, complexity, and data quality. Using technologies like Machine Learning (ML), Deep Learning (DL), Reinforcement Learning (RL), and Artificial Intelligence (AI), this research combines a lot of cutting-edge methods that work with Software-Defined Networking (SDN), the Internet of Things (IoT), and 5G environments. Using cutting-edge computer techniques, these works improve network security, traffic management, and communication protocols.

Each of the related work references focuses on a different aspect of network security while addressing these issues. Multiple layers of data and network protocols are used by researchers to fix problems with data quality and privacy, which makes the Internet of Things (IoT) safer (Restauccia et al., 2018). In a similar manner, Casas-Velasco et al. (2020) employ Reinforcement Learning (RL) in Software-Defined Networking (SDN) to address the challenges posed by complexity and enhance the efficiency of routing. Alzahrani et al. (2021) enhance the network security framework by rectifying data quality issues and employing machine learning to detect network attacks. These examples demonstrate the versatility of the contributions by presenting a range of innovative approaches to address issues such as intrusion prevention, anomaly detection, and enhancement of traffic flow and routing efficiency. The significance of this research lies in its potential to enhance our understanding of designing and implementing robust security protocols within intricate networked environments. Table 1 displays a comparison of various related works.

Table 1. Comparison for Related Works

Ref.	Challenges of			Motivation	Aim and Objective	Contribution	Achieved Results
	Data Quality	Privacy	Complexity				
[1]	✓	✓	✓	IoT Security	Enhancing Network Security	ML & SDN for IoT Safety	Improved IoT Safety
[2]	✗	✗	✓	SDN Routing Efficiency	Intelligent Routing using RL	Improved Routing Efficiency	Increased Efficiency
[3]	✓	✗	✓	Network Security Framework	ML for Attack Detection	Enhanced Security Framework	Identified Network Attacks
[4]	✗	✗	✓	Autonomous Defence	RL in SDN	Reinforcement Learning for Defence	Autonomous Defence
[5]	✗	✗	✓	Multimedia Traffic Control	Deep RL in SDN	Improved Traffic Control	Optimized Routing
[6]	✓	✗	✗	Flow-Based Anomaly Detection	ML Approach	Enhanced Anomaly Detection	Improved Anomaly Detection
[7]	✗	✓	✗	Drone Communication Security	ML & SDN for Drone Security	Secured Drone Communication	Enhanced Communication Security
[8]	✗	✗	✓	Multimedia Traffic Control	Deep RL in SDN	Optimized Traffic Control	Reduced Latency
[9]	✗	✗	✓	Mobile IoT Routing	ML Routing Protocol	Improved Routing in Mobile IoT	Enhanced Routing in Mobile IoT
[10]	✗	✗	✗	Software-Defined Wireless Networking	Innovative Architecture	SDN for Wireless Networking	Improved Wireless Networking
[11]	✗	✗	✗	Intrusion Detection in SDN	Deep Learning Approach	Improved Intrusion Detection	Enhanced Intrusion Detection
[12]	✗	✗	✗	Traffic Classification in SDN	ML & Deep Learning	Improved Traffic Classification	Enhanced Traffic Classification
[13]	✗	✗	✗	Traffic Classification	ML Algorithms	Comparative Analysis	Classification Optimization
[14]	✗	✗	✓	Traffic Prediction in SDN	Deep Learning	Optimized Routing Paths	Reduced Latency
[15]	✗	✗	✗	Network Traffic Discrimination	Deep Autoencoder	Improved Traffic Discrimination	Enhanced Traffic Discrimination
[16]	✗	✗	✗	Anomaly Detection in SDN	Deep Learning Approach	ML-Based Anomaly Detection	Enhanced Anomaly Detection
[17]	✗	✗	✗	Intrusion Detection in SDN	ML-Based IDS	Improved Intrusion Detection	Enhanced Intrusion Detection
[18]	✗	✗	✓	SDN Routing Optimization	Deep RL	Routing Optimization	Improved Routing
[19]	✗	✗	✗	Cognitive Routing Optimization	Deep ELM Approach	Intelligent Cognitive Routing	Optimized Routing
[20]	✗	✗	✗	Routing Optimization in SDN	DQN & Traffic Prediction	Improved Routing Optimization	Enhanced Routing Optimization
[21]	✗	✗	✗	Network Intelligent Control	SDN & AI	Traffic Optimization	Improved Traffic Control
[22]	✗	✗	✓	Content-Aware Traffic Engineering	AI-Driven Approach	Intelligent Traffic Engineering	Improved Routing Paths
[23]	✗	✗	✗	Intelligent Traffic Engineering	Machine Learning	Traffic Engineering Optimization	Improved Traffic Engineering
[24]	✗	✗	✓	Security Management in SDN-NFV	ML Empowered Security	Quality of Service Provision	Improved QoS Provision

[25]	✗	✗	✗	AI-Assisted Service Virtualization	Framework for 6G IoT	Service Management Framework	Efficient Flow Management
[26]	✓	✗	✗	Quality of Service Measurement	AI Technology	QoS Measurement and Prediction	Improved QoS Measurement
[27]	✗	✗	✗	Network Security in OpenStack	Scalable Security Framework	Security Framework for OpenStack	Enhanced Security for OpenStack
[28]	✗	✗	✓	DDoS Detection in SDN	Comparative Study	AI-Enabled DDoS Detection	Improved DDoS Detection
[29]	✗	✗	✗	5G Resource Introspection	Machine Learning	Dynamic Resource Allocation	Efficient Resource Allocation
[30]	✗	✗	✗	Resource Allocation in SDN-Fog	ML-Based Allocation Scheme	Efficient Resource Allocation	Optimized Resource Allocation
[31]	✗	✗	✗	Collision Flows Detection in 5G	ML Algorithms	Detection of Collision Flows	Identified Collision Flows
[32]	✗	✗	✗	Traffic Management in IoT	GNN & MAB	IoT Traffic Management	Improved Traffic Management
[33]	✗	✗	✗	Machine Learning in SDN	ML-Based Approach	Integration of ML in SDN	Enhanced ML Integration
[34]	✗	✗	✗	Secure IoT Architecture	Deep Learning & SDN	Security in IoT Architecture	Improved IoT Security
[35]	✗	✗	✗	Traffic Engineering Framework	ML-Based Meta-Layer	Improved Traffic Engineering	Enhanced Traffic Engineering
[36]	✗	✓	✗	DDoS Attack Detection	ML Algorithms	Detection of DDoS Attacks	Identified DDoS Attacks
[37]	✗	✗	✗	DDoS Attack Detection in SDN	Hybrid ML Techniques	Detection of DDoS Attacks	Identified DDoS Attacks
[38]	✗	✗	✗	Intrusion Detection in SDN	ML-Based IDS	Improved Intrusion Detection	Enhanced Intrusion Detection
[39]	✗	✗	✗	IDS in SDN	ML Approach	Survey on IDS	Enhanced IDS Survey
[40]	✗	✗	✗	Preventing DDoS Attack	Intelligent SDN Controller	Prevention of DDoS Attacks	Reduced DDoS Attacks
[41]	✗	✗	✗	Tracing DoS Attack in SDN	ML-Based Tracing	Dynamic Tracing of DoS Attacks	Enhanced Tracing of DoS Attacks
[42]	✗	✗	✗	Link Congestion Prediction	ML for SDN Data Plane	Prediction of Link Congestion	Reduced Congestion
[43]	✗	✗	✗	Traffic Tolerance Improvement	ML-Aided Traffic Tolerance	Improved Resilience	Enhanced Traffic Resilience
[44]	✗	✗	✓	Mobile Metro-Core Networks	Matheuristic & ML-Based Prediction	Optimization in Mobile Networks	Improved Optimization
[45]	✗	✗	✗	DDoS Attack Detection in SDN	ML Algorithms	Detection of DDoS Attacks	Identified DDoS Attacks
[46]	✗	✗	✗	Data Collection in SDN	ML & Traffic Classification	Data Collection and Classification	Improved Data Handling

The checkmarks (✓) indicate that the paper addresses the corresponding aspect, while crosses (✗) indicate that the aspect is not specific.

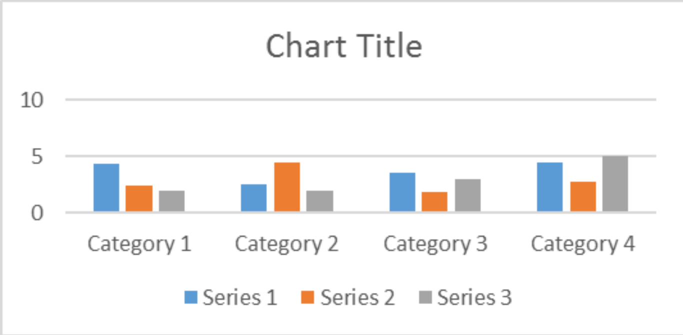

Figure1. Title [Cambria 12, space single, format png/jpg]

F. Conclusion

The amalgamation of artificial intelligence and machine learning is augmenting the functionalities of software-defined networking (SDN) in network optimization, anomaly detection, and traffic prediction. Given their capacity to adapt to changing network conditions and enhance performance, they have a vital role in modern network management. Ultimately, the analysis of all the sources yielded a thorough understanding of the operation of machine learning and artificial intelligence (AI) in software-defined networking (SDN). The application of Artificial Intelligence (AI) and Machine Learning (ML) in Software-Defined Networking (SDN) showcases their effectiveness in tackling complex problems and improving network security. These applications are especially noticeable in areas such as traffic forecasting, anomaly identification, network enhancement, and other fields. These technologies improve the effectiveness and adaptability of SDN configurations by streamlining traffic management and optimizing resource allocation in the field of traffic prediction. Various studies have shown that the application of deep learning and machine learning algorithms greatly improves the identification of anomalies, which is crucial for detecting security issues. Despite ongoing concerns about complexity, privacy, and data quality, the observed modifications are a promising indication. These studies enhance our understanding of network security and provide valuable insights into the current strategies used to tackle these problems. These research projects are highly significant as they have the potential to completely transform future network security protocols and develop groundbreaking methods to improve the robustness, adaptability, and security of network infrastructures.

G. References

[1] Restuccia, F., D'Oro, S., & Melodia, T. (2018). Securing the internet of things in the age of machine learning and software-defined networking. IEEE Internet of Things Journal, 5(6), 4829-4842.

[2] Tua Halomoan Harahap, Sofiene Mansouri, Omar Salim Abdullah, Herlina Uinarni, Shavan Askar, Thaer L. Jabbar, Ahmed Hussien Alawadi, Aalaa Yaseen Hassan, An artificial intelligence approach to predict infants' health status at birth, International Journal of Medical Informatics, Volume 183, 2024, 105338, ISSN 1386-5056,

[3] Casas-Velasco, D. M., Rendon, O. M. C., & da Fonseca, N. L. (2020). Intelligent routing based on reinforcement learning for software-defined networking. IEEE Transactions on Network and Service Management, 18(1), 870-881.
[4] Alzahrani, A. O., & Alenazi, M. J. (2021). Designing a network intrusion detection system based on machine learning for software defined networks. Future Internet, 13(5), 111.
[5] Arif Sari, Candra Zonyfar, Shavan Askar, Sherzod Abdullaev, Raaid Alubady, M. K. Sharma, "An embedded machine learning strategy for analyzing interfacial characteristics in impact welding of dissimilar alloys" Composite Interfaces , 2023.
[6] Itika Sharma, Sachin Kumar Gupta, Ashutosh Mishra, Shavan Askar, "Synchronous Federated Learning based Multi Unmanned Aerial Vehicles for Secure Applications" Scalable Computing: Practice and Experience, Volume 2, No. 3, 2023.
[7] Diana Hayder Hussein; Shavan Askar, "Federated Learning Enabled SDN for Routing Emergency Safety Messages (ESMs) in IoV Under 5G Environment", IEEE Access, Volume 11, 2023.
[8] Han, Y., Rubinstein, B. I., Abraham, T., Alpcan, T., De Vel, O., Erfani, S., ... & Montague, P. (2018). Reinforcement learning for autonomous defence in software-defined networking. In Decision and Game Theory for Security: 9th International Conference, GameSec 2018, Seattle, WA, USA, October 29–31, 2018, Proceedings 9 (pp. 145-165). Springer International Publishing.
[9] Yu, C., Lan, J., Guo, Z., & Hu, Y. (2018). DROM: Optimizing the routing in software-defined networks with deep reinforcement learning. IEEE Access, 6, 64533-64539.
[10] Dey, S. K., & Rahman, M. M. (2019). Effects of machine learning approach in flow-based anomaly detection on software-defined networking. Symmetry, 12(1), 7.
[11] Guerber, C., Royer, M., & Larrieu, N. (2021). Machine Learning and Software Defined Network to secure communications in a swarm of drones. Journal of information security and applications, 61, 102940.
[12] Huang, X., Yuan, T., Qiao, G., & Ren, Y. (2018). Deep reinforcement learning for multimedia traffic control in software-defined networking. IEEE Network, 32(6), 35-41.
[13] R. Samadi and J. Seitz, "Machine Learning Routing Protocol in Mobile IoT based on Software-Defined Networking," 2022 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Phoenix, AZ, USA, 2022, pp. 108-111, doi: 10.1109/NFV-SDN56302.2022.9974791.
[14] Bernardos, C. J., et al. (2014). An architecture for software-defined wireless networking. IEEE Wireless Communications, 21(3), 52-61.
[15] Media Ali Ibrahim; Shavan Askar, "An Intelligent Scheduling Strategy in Fog Computing System Based on Multi-Objective Deep Reinforcement Learning Algorithm", IEEE Access, Volume 11, 2023.
[16] Saman M. Omer, Kayhan Z. Ghafoor & Shavan K. Askar , "Lightweight improved yolov5 model for cucumber leaf disease and pest detection based on deep learning" Journal of Signal, Image and Video Processing, 2023

[17] Omar Shirko; Shavan Askar , “A Novel Security Survival Model for Quantum Key Distribution Networks Enabled by Software-Defined Networking” IEEE Access, Volume 11, 2023.
[18] Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A. R., Ghogho, M., & El Moussa, F. (2020). DeepIDS: Deep Learning Approach for Intrusion Detection in Software Defined Networking. Electronics, 9(9), 1533. MDPI AG. Retrieved from http://dx.doi.org/10.3390/electronics9091533.
[19] Mohammed, A. R., Mohammed, S. A., & Shirmohammadi, S. (2019). Machine Learning and Deep Learning Based Traffic Classification and Prediction in Software Defined Networking. In 2019 IEEE International Symposium on Measurements & Networking (M&N) (pp. 1-6). Catania, Italy. DOI: 10.1109/IWMN.2019.8805044.
[20] Tonkal, Ö. & Polat, H. (2021). Traffic Classification and Comparative Analysis with Machine Learning Algorithms in Software Defined Networks . Gazi University Journal of Science Part C: Design and Technology , 9 (1) , 71-83 . DOI: 10.29109/gujsc.869418.
[21] R. Xiong, Q. Yuan, H. Zhang, X. Wang and K. Ma, "Deep Learning Traffic Prediction to Optimize Routing Paths and Reduce Latency in SDN," 2023 IEEE 6th International Conference on Industrial Cyber-Physical Systems (ICPS), Wuhan, China, 2023, pp. 1-7, doi: 10.1109/ICPS58381.2023.10128099.
[22] Dezheen H. Abdulazeez; Shavan K. Askar, “Offloading Mechanisms Based on Reinforcement Learning and Deep Learning Algorithms in the Fog Computing Environment” IEEE Accesss Volume 11, 2023.
[23] Saman M. Omer, Kayhan Z. Ghafoor, Shavan K. Askar, “Plant Disease Diagnosing Based on Deep Learning Techniques” ARO journal, 2022.
[24] Saman M. Omer, Kayhan Z. Ghafoor, Shavan K. Askar, “An Intelligent System for Cucumber Leaf Disease Diagnosis Based on the Tuned Convolutional Neural Network Algorithm” Journal of Mobile Information systems, Volume 2022.
[25] Shirmarz, A., & Ghaffari, A. (2023). Network traffic discrimination improvement in software defined network (SDN) with deep autoencoder and ensemble method. Journal of Ambient Intelligence and Humanized Computing, 14(5), 6321-6337.
[26] Qin, Y., Wei, J., & Yang, W. (2019, September). Deep learning based anomaly detection scheme in software-defined networking. In 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS) (pp. 1-4). IEEE.
[27] Abubakar, A., & Pranggono, B. (2017, September). Machine learning based intrusion detection system for software defined networks. In 2017 seventh international conference on emerging security technologies (EST) (pp. 138-143). IEEE.
[28] Stampa, G., Arias, M., Sánchez-Charles, D., Muntés-Mulero, V., & Cabellos, A. (2017). A deep-reinforcement learning approach for software-defined networking routing optimization. arXiv preprint arXiv:1709.07080.
[29] Alhaidari, F., Almotiri, S. H., Al Ghamdi, M. A., Khan, M. A., Rehman, A., Abbas, S., ... & Rahman, A. U. (2021). Intelligent software-defined network for cognitive routing optimization using deep extreme learning machine approach. Computers, Materials & Continua, 67(1), 1269-1285.

[30] Bouzidi, E. H., Outtagarts, A., Langar, R., & Boutaba, R. (2021). Deep Q-Network and traffic prediction based routing optimization in software defined networks. Journal of Network and Computer Applications, 192, 103181.

[31] Guo, A., & Yuan, C. (2021). Network intelligent control and traffic optimization based on SDN and artificial intelligence. Electronics, 10(6), 700.

[32] Q. Zhang, X. Wang, J. Lv and M. Huang, "Intelligent Content-Aware Traffic Engineering for SDN: An AI-Driven Approach," in IEEE Network, vol. 34, no. 3, pp. 186-193, May/June 2020, doi: 10.1109/MNET.001.1900340.

[33] Andrushchak, V., Beshley, M., Dutko, L., Maksymyuk, T., Andrukhiv, T. (2022). Intelligent Traffic Engineering for Future Intent-Based Software-Defined Transport Network. In: Klymash, M., Beshley, M., Luntovskyy, A. (eds) Future Intent-Based Networking. Lecture Notes in Electrical Engineering, vol 831. Springer, Cham. https://doi.org/10.1007/978-3-030-92435-5_9.

[34] Shahzadi, S., Ahmad, F., Basharat, A., Alruwaili, M., Alanazi, S., Humayun, M., ... & Naseem, S. (2021). Machine learning empowered security management and quality of service provision in SDN-NFV environment. Comput. Mater. Contin, 66(3), 2723-2749.

[35] Manogaran, G., Baabdullah, T., Rawat, D. B., & Shakeel, P. M. (2021). AI-assisted service virtualization and flow management framework for 6G-enabled cloud-software-defined network-based IoT. IEEE Internet of Things Journal, 9(16), 14644-14654.

[36] Lai, Y.-C., Kao, C.-C., Jhan, J.-D., Kuo, F.-H., Chang, C.-W., & Shih, T.-C. (2020). Quality of Service Measurement and Prediction through AI Technology. In 2020 IEEE Eurasia Conference on IoT, Communication and Engineering (ECICE) (pp. 254-257). Yunlin, Taiwan. https://doi.org/10.1109/ECICE50847.2020.9302008.

[37] Krishnan, P., Jain, K., Aldweesh, A., et al. (2023). OpenStackDP: A Scalable Network Security Framework for SDN-based OpenStack Cloud Infrastructure. Journal of Cloud Computing, 12(1), 26. https://doi.org/10.1186/s13677-023-00406-w

[38] Ko, K.-M., Baek, J.-M., Seo, B.-S., & Lee, W.-B. (2023). Comparative Study of AI-Enabled DDoS Detection Technologies in SDN. Applied Sciences, 13(17), 9488. MDPI AG. Retrieved from http://dx.doi.org/10.3390/app13179488.

[39] D. Basu, S. Kal, U. Ghosh and R. Datta, "DRIVE: Dynamic Resource Introspection and VNF Embedding for 5G Using Machine Learning," in IEEE Internet of Things Journal, vol. 10, no. 21, pp. 18971-18979, 1 Nov.1, 2023, doi: 10.1109/JIOT.2023.3235382.

[40] Singh, J., Singh, P., Hedabou, M., & Kumar, N. (2023). An Efficient Machine Learning-Based Resource Allocation Scheme for SDN-Enabled Fog Computing Environment. IEEE Transactions on Vehicular Technology, 72(6), 8004-8017. doi:10.1109/TVT.2023.3242585.

[41] Askar, Shavan and Keti, Faris, Performance Evaluation of Different SDN Controllers: A Review (July 14, 2021). IJSB Volume: 5, Issue: 6 Year: 2021 Page: 67-80, Available at SSRN: https://ssrn.com/abstract=3886086

[42] Shavan Askar & Kurdistan Ali & Tarik A. Rashid, 2021. "Fog Computing Based IoT System: A Review," International Journal of Science and Business, IJSAB International, vol. 5(6), pages 183-196.
[43] Shavan Askar & Zhala Jameel Hamad & Shahab Wahhab Kareem, 2021. "Deep Learning and Fog Computing: A Review," International Journal of Science and Business, IJSAB International, vol. 5(6), pages 197-208.
[44] Aqdus, A., Amin, R., Ramzan, S., Alshamrani, S. S., Alshehri, A., & El-kenawy, E. S. M. (2023). Detection Collision Flows in SDN Based 5G Using Machine Learning Algorithms. Computers, Materials & Continua, 75(1).
[45] Guo, Y., Wang, Y., Khan, F., Al-Atawi, A. A., Abdulwahid, A. A., Lee, Y., & Marapelli, B. (2023). Traffic Management in IoT Backbone Networks Using GNN and MAB with SDN Orchestration. Sensors, 23(16), 7091. MDPI AG. Retrieved from http://dx.doi.org/10.3390/s23167091
[46] Chnar Mustaf Mohammed & Shavan Askar, 2021. "Machine Learning for IoT HealthCare Applications: A Review," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 42-51.
[47] Kurdistan Ali & Shavan Askar, 2021. "Security Issues and Vulnerability of IoT Devices," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 101-115.
[48] Glena Aziz Qadir & Shavan Askar, 2021. "Software Defined Network Based VANET," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 83-91.
[49] J. Liu and Q. Xu, "Machine Learning in Software Defined Network," 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 2019, pp. 1114-1120, doi: 10.1109/ITNEC.2019.8729331.
[50] Dawoud, A., Shahristani, S., & Raun, C. (2018). Deep learning and software-defined networks: Towards secure IoT architecture. Internet of Things, 3, 82-89.
[51] L. Yanjun, L. Xiaobo and Y. Osamu, "Traffic engineering framework with machine learning based meta-layer in software-defined networks," 2014 4th IEEE International Conference on Network Infrastructure and Digital Content, Beijing, China, 2014, pp. 121-125, doi: 10.1109/ICNIDC.2014.7000278.
[52] N. Meti, D. G. Narayan and V. P. Baligar, "Detection of distributed denial of service attacks using machine learning algorithms in software defined networks," 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, India, 2017, pp. 1366-1371, doi: 10.1109/ICACCI.2017.8126031.
[53] V. Deepa, K. M. Sudar and P. Deepalakshmi, "Detection of DDoS Attack on SDN Control plane using Hybrid Machine Learning Techniques," 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2018, pp. 299-303, doi: 10.1109/ICSSIT.2018.8748836.
[54] G. Abhilash and G. Divyansh, "Intrusion Detection and Prevention in Software Defined Networking," 2018 IEEE International Conference on Advanced

Networks and Telecommunications Systems (ANTS), Indore, India, 2018, pp. 1-4, doi: 10.1109/ANTS.2018.8710141.
[55] P. Vaid, S. K. Bhadu and R. M. Vaid, "Intrusion detection system in Software defined Network using machine learning approach - Survey," 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatre, India, 2021, pp. 803-807, doi: 10.1109/ICCES51350.2021.9489141.
[56] A. Prakash and R. Priyadarshini, "An Intelligent Software defined Network Controller for preventing Distributed Denial of Service Attack," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 2018, pp. 585-589, doi: 10.1109/ICICCT.2018.8473340.
[57] A. Chopra and D. C. Verma, "Dynamic Tracing of DoS Attack Over Software-Defined Networks Using Machine Learning," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 635-640, doi: 10.1109/PDGC56933.2022.10053364.
[58] J. Wu, Y. Peng, M. Song, M. Cui and L. Zhang, "Link Congestion Prediction using Machine Learning for Software-Defined-Network Data Plane," 2019 International Conference on Computer, Information and Telecommunication Systems (CITS), Beijing, China, 2019, pp. 1-5, doi: 10.1109/CITS.2019.8862098.
[59] S. Gangadhar and J. P. G. Sterbenz, "Machine learning aided traffic tolerance to improve resilience for software defined networks," 2017 9th International Workshop on Resilient Networks Design and Modeling (RNDM), Alghero, Italy, 2017, pp. 1-7, doi: 10.1109/RNDM.2017.8093035.
[60] R. Alvizu, S. Troia, G. Maier and A. Pattavina, "Matheuristic with machine-learning-based prediction for software-defined mobile metro-core networks," in Journal of Optical Communications and Networking, vol. 9, no. 9, pp. D19-D30, Sept. 2017, doi: 10.1364/JOCN.9.000D19.
[61] Zhala Jameel Hamad & Shavan Askar, 2021. "Machine Learning Powered IoT for Smart Applications," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 92-100.
[62] Kosrat Dlshad Ahmed & Shavan Askar, 2021. "Deep Learning Models for Cyber Security in IoT Networks: A Review," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 61-70
[63] S. Sanapala, D. D. Reddy, G. L. Chowdary and K. S. Vikyath, "Machine Learning Based DDoS Attack Detection in Software Defined Networks (SDN)," 2023 2nd International Conference on Edge Computing and Applications (ICECAA), Namakkal, India, 2023, pp. 1124-1126, doi: 10.1109/ICECAA58104.2023.10212147.
[64] P. Amaral, J. Dinis, P. Pinto, L. Bernardo, J. Tavares and H. S. Mamede, "Machine Learning in Software Defined Networks: Data collection and traffic classification," 2016 IEEE 24th International Conference on Network Protocols (ICNP), Singapore, 2016, pp. 1-5, doi: 10.1109/ICNP.2016.7785327.