Anusandhanvallari
Vol 2025, No.1
August 2025
ISSN 2229-3388

Advanced Techniques for Secure and Efficient SDN Management a Survey

Mrs. K. Priyadharshini[1], Dr. S. Devaraju[2], Dr. B. Radha [3]
Computer science, Sri Krishna Arts and Science College, Bharathiar University, India.
E-mail: priya95joy@gmail.com
Computer science, VIT Bhopal University, India.
E-mail: devamcet@gmail.com
Computer science, Sri Krishna Arts and Science College, Bharathiar University, India.
E-mail: radhab@skasc.ac.in

Abstract : Software-Defined Networking (SDN) has revolutionized network management by decoupling the control plane from the data plane, offering dynamic, programmable, and centralized network control. However, the complexity and scale of modern networks demand advanced techniques for secure and efficient SDN management. This survey explores cutting-edge methodologies, technologies, and strategies aimed at enhancing the security and efficiency of SDN infrastructures. The survey begins by examining security challenges in SDN environments, such as controller vulnerabilities, network attacks, and data privacy concerns. It then delves into security-enhancing techniques like access control mechanisms, encryption protocols, anomaly detection, and threat intelligence integration, providing insights into how these methods mitigate risks and fortify SDN infrastructures against cyber threats. On the efficiency front, the survey explores optimization techniques for resource allocation, traffic engineering, and Quality of Service (QoS) provisioning in SDN networks. It covers topics like network slicing, load balancing algorithms, dynamic routing strategies, and bandwidth management solutions, showcasing how these approaches enhance network performance, scalability, and resource utilization. Furthermore, the survey highlights emerging trends such as Artificial Intelligence (AI) and Machine Learning (ML) applications in SDN security and management, discussing their potential to automate threat detection, optimize network operations, and adaptively respond to evolving network conditions.

Keywords: Access control mechanisms, Centralized control, Dynamic control, Network attacks, Software-Defined Networking

I. Introduction

A revolutionary change in network design, software-defined networking (SDN) allows for programmable and dynamic network administration. Routers and switches are the typical nodes in a network that perform both control plane and data plane tasks in conventional networking. SDN decouples these tasks, with a single administrator overseeing the data plane devices and the network's control plane [1–5]. SDN allows administrators to programmatically manage the behaviour of networks using software applications by operating on the premise of separating network control and forwarding operations [6-7]. Thanks to its adaptability and programmability, network administration, scalability, and agility have seen tremendous improvements [8–10].

Ensuring the security and integrity of SDN environments relies heavily on anomaly detection [11, 12]. An anomaly detection technique can spot suspicious or harmful activity on a network by keeping a close eye on its traffic and behaviour patterns in real time [13–14]. Protecting SDN infrastructures relies heavily on secure authentication and access control systems [15-16]. To prevent unauthorised parties from making changes to configuration settings or gaining access to critical network resources, these systems verify the identity of devices or users trying to connect to the network and implement rules to restrict access [17–18]. In software-defined networking (SDN), "link quality" is defined as the dependability, efficiency, and accessibility of the network connections that link SDN nodes [19, 20]. To optimize network performance, minimize latency, and ensure reliable data transfer, efficient link quality control is necessary [21-25]. There is an increasing need to

resolve issues with anomaly detection, secure authentication, access control, and connection quality management as SDN develops further. Network management and cybersecurity academics, practitioners, and decision-makers might benefit from this survey's examination of cutting-edge approaches to improving SDN environments' security, efficiency, and dependability [26-30].

II. Literature survey

Abdi, A. et al. (2024) Software-defined networking (SDN) was a new way of thinking about networking that separates the data plane from the control plane. This makes it much easier to modify and adapt programmes, which was especially useful in data centres. On the other hand, programmable data planes and centralized control were appealing targets for bad actors, therefore this separation creates a number of security issues.

Abdulqadder, I. et al. (2018) To protect against flow table overloading, control plane saturation, and Byzantine assaults, the author provide a SecSDN-cloud architecture. By using SHA3-384, the Digital Signature with a Chaotic Secure Hashing (DS-CSH) was able to handle the need for user authentication. User packets were not subject to examination based on predefined regulations until the user has been validated. The cloud server that oversees monitoring defines policies according on packet characteristics.

Alidadi, A. et al. (2022) This research introduced a new approach to restricted bandwidth routing based on data from Path Computing Element (PCE) nodes. Links were chosen to fulfil the largest number of future needs using the link weight established in this study. The efficacy of the novel strategy was evaluated using the results of the simulation. When compared to other approaches, the author discovered that Path Selection with Low Complexity (PSLC) performs the best. Both the importance of key connections and their relative importance for routing viable LSP setup requirements were checked by these authors newly presented technique.

Aliyu, A. et al. (2020) There was a security risk in the SDN architecture between the controller and the network applications, and the suggested trust framework was an attempt to fix it. In this study, the author take the trust framework's design concept and abstract ideas and turn them into a testable, implementable enhance. In order to authenticate network applications running on the Network Function Virtualization layer and provide them the appropriate privileges, the suggested trust framework provides mechanisms for doing so.

Anitha, H. et al. (2024) In order to access the virtual machines in the cloud, SDN-enabled role-based secret sharing was put into place. Virtual machines (VMs) in the cloud were vulnerable to attacks that occur while the user was interacting with them. The VMs were protected against assaults thanks to the implementation of SDN enabled role based secret sharing scheme (SRBSSS). Carefully avoiding the environment's untrusted users was the approach's main goal. This ensures that security attributes like availability, secrecy, and integrity were preserved. In the cloud, resources were not withheld from legitimate users. Rather of dealing with assaults after they have occurred, it was preferable to prevent them. The secret key was generated at random by the SDN controller and was unknown to all parties involved.

Cho, J. Y., & Szyrkowiec, T. (2018) The author provide an access control mechanism and a hash-based authentication method that can safeguard an SDN-based optical network against optical security risks in this study. The Merkle hash tree, constructed entirely from cryptographic hash functions, was the basis of the suggested procedures. Therefore, the suggested methods do not need computationally costly procedures for deployment on optical network devices.

Golightly, L. et al. (2023) The author analyzed the most cutting-edge Access Control systems now in use by businesses as a cybersecurity strategy for authorizing users and data throughout this study. In particular, the author assessed the benefits and drawbacks of new solutions by looking at a range of contemporary application fields including cloud computing, the IoT, Blockchain, and Software-Defined Networking (SDN).

Ibrahim, A. et al. (2022) In order to achieve efficient routing and energy savings in SDN, this article discusses energy awareness in dispersed network topologies. Saving energy was the golden rule in distributed

systems when it comes to controller placement and load balancing among connections. Network parts must be able to communicate with one another in order to reduce route length in an SDN framework, which was not an easy task. To make the most of SDN's potential for energy savings, the author have included controllers for a distributed control plane in this effort. Therefore, the goal of the energy-aware algorithm was to maximize efficiency while minimizing power consumption and uneven load distribution.

Iqbal, M. et al. (2019) The need for reliable, adaptable, and well-managed networks has been met with the advent of software-defined networks. However, there were more attack vectors in SDN than in conventional networks since the two planes were separated. This implies that control and network traffic might be severely compromised in terms of availability, consistency, authenticity, secrecy, and integrity. Some of the most fundamental dangers to the SDN were detailed in this article, along with some of the proposed remedies.

Islam, M. J. (2020) Standards for administration and well-being were still in the works, and the technology behind the IoT and SDN was still in its infancy. A small number of academics have tackled specific issues with SDN-IoT. The authors have presented a secure SDN-IoT paradigm for smart cities using NFV, with that idea at its core. There were a number of distributed controllers that have proposed improvements to security, management, availability, secrecy, safety, authentication, policy implementation, and mitigation.

Jain, A. et al. (2023) There was a lot of data, yet DPI in SDN was still low. Despite the availability of third-party DPI solutions, this paper proposes a groundbreaking approach to SDN using machine learning methods called Stacked Autoencoder Based Convolutional Neural Networks (SA-CNN).

Kanwal, A. et al. (2024) Several proposals have been put forth to strengthen and protect the SDN controller, which was mission-critical software responsible for managing the whole network. Some research has looked at using permission-based access control to secure SDN assets within the framework of individual SDN controllers, but this hasn't backed up the idea of automated and flexible access control for SDN assets. These authors research was an ancillary effort that aims to mechanise some of the laborious processes used in earlier studies.

Kanwal, A. et al. (2024) A new paradigm for managing heterogeneous networks, software-defined networking has arisen and was revolutionizing network-working technologies. These networks can range from modest residences to large business networks. New ways to identify and mitigate different threats can be implemented via the programmability and logically centralized and distributed control plane of the SDN paradigm, which also enables security as a service. This presents a huge potential to enhance network security. On the other hand, security issues abound at every level of SDN.

Kim, J. et al. (2024) In this study, the author have reviewed all aspects of SDN security, including potential threats and countermeasures. Among these authors contributions were new taxonomies that categories things according to their origins and penetration pathways. The author have arranged current assaults in a hierarchical structure according to the many levels of defence and penetration paths. The author have highlighted crucial areas that need further attention after thoroughly investigating motives, methods, and basic security concerns.

Mendiboure, L. et al. (2020) An efficient method of configuring Software Defined Vehicular Networking (SDVN's) authentication and access control might be blockchain. In fact, it ensures cheap prices, great flexibility, and a high degree of safety. Two major issues with current Blockchain-based solutions were their inability to authenticate or regulate access to SDN controllers and their inadequate scalability for big SDVNs.

Mhamdi, L., & Isa, M. M. (2024) In order to identify intrusions in a native SDN environment, this article introduced a Deep AutoEncoder with a Random Forest (DAERF) Machine learning model, which was a blend of AutoEncoder and Random Forest. The author demonstrated that the suggested DAERF outperforms prior efforts with a 98% accuracy and reduced training and execution times. Positively, the findings demonstrate that the model was effective at detecting intrusions in real-time.

Midha, S. et al. (2023) The Remote Health Monitoring System (RHMS) makes it easy to treat patients whenever and wherever they need it. Greater scalability and flexibility were available for patient data stored on the cloud-based SDN server. Maintaining the confidentiality of patients' personal information remains a significant challenge due to security concerns. Poor health management might result from a breach of patients' personal information. Each transaction's biometric imprint, nonce, and timestamp computation ensure that keys remain fresh and data remains intact under these authors proposed protocol.

Mutaher, H., & Kumar, P. (2021) In a software-defined network, the policies and regulations of the network were obtained via communication between the controller and a large number of hosts. Administrators of the network must verify all hosts in order to keep the network from collapsing due to the large number of hosts. To ensure that the hosts were legitimate in the eyes of the controller, this article suggests an authentication method.

Patwary, A. et al. (2021) The primary goal of this research was to identify potential security vulnerabilities in the Fog computing platform by reviewing, investigating, and analyzing its concerns. There were a lot of security concerns that need be thought about, and they don't exist in the standard cloud computing setting. There must also be major advancements in the Fog setting. By compiling all security features of the Fog computing paradigm—including authentication, access control, privacy preservation, trust management, threats, assaults, and security auditing—the author address a vacuum in the existing literature.

Rzym, G. et al. (2024) Anomaly detection in computer networks was becoming partially automated, and this article offers a major approach in machine learning to solve this. A careful comparison was made between two scenarios that used different time periods for data collecting.

Table 1: Comparison table for approaches in SDN Security and Anomaly Detection

Author	Year	Methodology	Advantage	Limitation
Rzym et al.	2024	Utilization of dynamic telemetry and deep neural networks for anomaly detection in 6G SDN	Integration of advanced technologies for anomaly detection, potential for accurate and timely threat identification	Limited discussion on scalability, resource requirements for deep learning models
Sallam et al.	2019	Development of a secure and scalable SDN framework using the software-defined perimeter approach	Scalability and scalability of the proposed SDN framework, enhanced security through a perimeter-based approach	Lack of extensive empirical validation, potential overhead of implementing a new framework
Songa & Karri,	2024	Integration of an SDN framework for early detection of DDoS attacks in cloud computing	Early detection capabilities for DDoS attacks, integration with cloud environments for comprehensive threat mitigation	Limited discussion on resource utilization, applicability to diverse cloud environments
Yue et al.	2020	DoS attack detection based on multi-feature analysis in SDN	Multi-feature analysis for robust DoS attack detection, potential for identifying complex attack patterns	Specific focus on DoS attacks, can overlook other types of network threats

III. Existing Methods

3.1 Popular methods

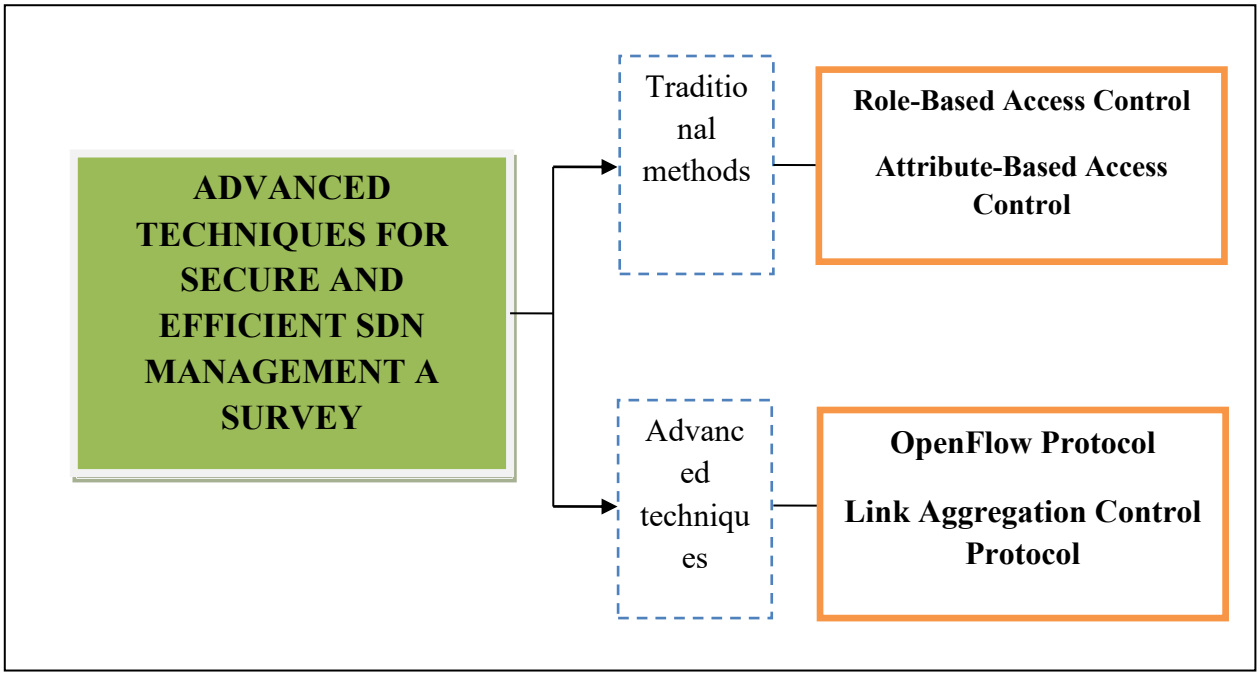

Figure 1: Traditional and Advanced techniques

Table 2: comparison table for existing methods

Algorithm	Merits	Demerits
Attribute-Based Access Control	Using ABAC, access control rules can be fine-grained according to a variety of criteria, including user roles, characteristics, resource attributes, and even environmental variables. With this level of detail, can manage who has access to what resources and under what circumstances. By consolidating policy management and decreasing the need for manual modifications to access control rules, ABAC streamlines the administration of access controls.	It can be challenging to design and apply ABAC rules in settings with many qualities and complicated interactions between them. Using ABAC to its full potential can need access control policy design and administration skills for some organizations.
Role-Based Access Control	By grouping permissions according to predetermined roles instead of individual users, RBAC streamlines the administration of access controls. This streamlines the process of managing access rights in big organizations while	Role bloat, in which the number of roles increases dramatically, can make role administration difficult and time-consuming in complicated setups with many permissions and responsibilities. This phenomenon is known as role explosion.

	reducing administrative costs.	
eXtensible Access Control Markup Language	By letting users, resources, environments, and actions specify access rules based on a variety of properties, XACML makes fine-grained access control possible. With this level of detail, it is possible to regulate precisely which users have access to which resources and under what circumstances.	The need to evaluate attributes, make policy decisions, and enforce policies can lead to performance overhead in XACML implementations. The system's performance can be affected by rules that are either complicated or have a high number of assessments.
Link Aggregation Control Protocol	Among LACP's many benefits is the ability to consolidate several physical connections between devices in a network into a single logical one. A greater throughput for data transport is made possible by increasing the available bandwidth via this aggregation.	Users without extensive networking experience can find the process of setting up and configuring LACP to be particularly daunting. A thorough familiarity with LACP characteristics, modes (passive or active), and hardware compatibility is necessary for correct setup.

3.2 Role-Based Access Control

By classifying users into predefined roles such as "Administrator," "Manager," or "Employee," with predefined permissions, Role-Based Access Control (RBAC) simplifies access management by separating users with similar responsibilities into these roles. Enhancing security by lowering the possibility of privilege abuse, RBAC implements the concept of least privilege by allowing users just the minimal access essential for their job tasks. The ability to centrally manage access control rules ensures uniformity, compliance, and auditability across the organisation, while dynamic job assignment helps with responsiveness to changing demands.

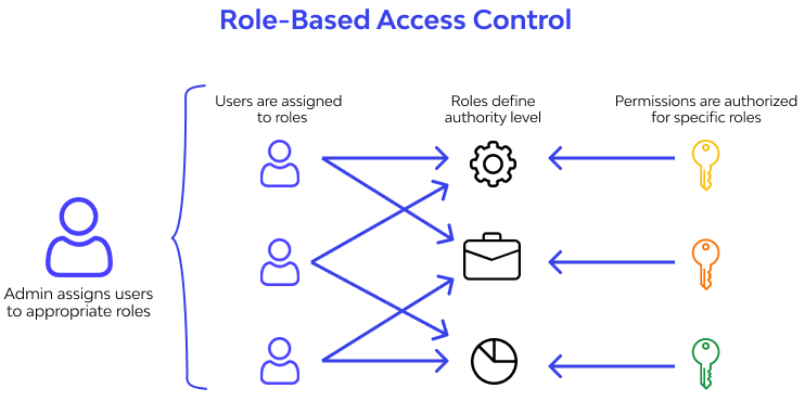

Figure 1: **Role-Based Access Control [Source: https://www.wallarm.com/what/what-exactly-is-role-based-access-control-rbac]**

3.3 OpenFlow Protocol

Software-Defined Networking (SDN) designs make it possible to programme and centrally manage network devices via the use of the OpenFlow protocol, a standardized communication protocol. It divides the network into two distinct planes, one for controlling packet forwarding and the other for actually forwarding the data. The OpenFlow protocol allows a network's central controller to dynamically adjust forwarding rules and policies via communication with routers and switches. A more versatile, scalable, and adaptive network can be achieved when administrators are able to centrally design and regulate the network's behaviour. OpenFlow makes it easier to automate processes, optimize networks, engineer traffic, and build new network services and apps. It has become an essential part of current software-defined networking (SDN) installations, allowing for more flexibility and programmability in network administration.

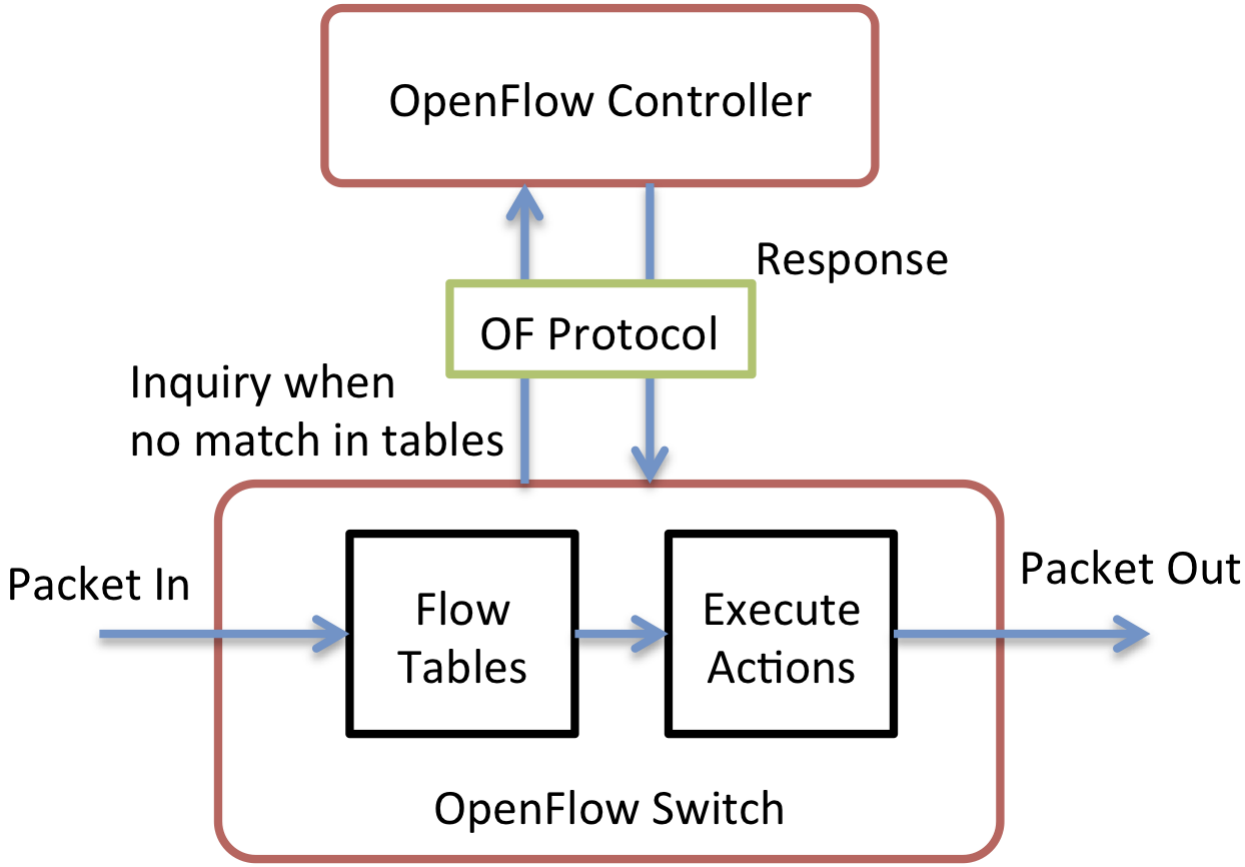

Figure 2: OpenFlow Protocol [Source: https://medium.com/@fiberoptics/openvswitch-and-openflow-what-are-they-whats-their-relationship-d0ccd39b9a5c]

3.3 Automated Link Recovery

Restoring network connection and functioning after a link loss or deterioration automatically, without operator intervention, is called Automated Link Recovery. To ensure high availability and uninterrupted communication in network environments, this mechanism uses protocols like Automatic Link Aggregation (ALA), Bidirectional Forwarding Detection (BFD), Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Virtual Router Redundancy Protocol (VRRP), Hot Standby Router Protocol (HSRP), and Link Aggregation. It is particularly important in dynamic and Software-Defined Networking (SDN) architectures where adaptive network behaviour is critical.

IV. Discussion

Examining the many facets of Software-Defined Networking (SDN), this review recognizes the revolutionary effect SDN has had on network administration and tackles the complicated problems it causes, especially with regard to efficiency and security. In order to strengthen SDN infrastructures against cyber threats, the survey first analyses security vulnerabilities like controller exploits, network attacks, and data privacy issues. Then, it discusses advanced security techniques like encryption protocols, anomaly detection, access control mechanisms, and threat intelligence integration. Optimal resource allocation, traffic engineering, Quality of Service (QoS) provisioning, and new technology that can automate threat detection, optimize network operations, and adapt to changing network demands are all topics covered in the survey as it delves into the world of SDN efficiency optimization. In today's ever-changing networking landscapes, it is crucial to use state-of-the-art approaches and technologies for SDN deployments to be safe, robust, and efficient.

V. Conclusion

Ultimately, the study highlights the paramount significance of strong security protocols and effective management approaches in SDN settings. To better protect their SDN infrastructures from ever-changing cyber threats, organizations should tackle the security issues that come with SDN, such as network attacks and controller vulnerabilities, and look into security-enhancing techniques, such as encryption protocols, access control, anomaly detection, and threat intelligence integration. At the same time, organizations can improve their network operations' responsiveness, scalability, and agility by optimizing efficiency through traffic engineering, Quality of Service (QoS) provisioning, and resource allocation. They can also harness the power of emerging technologies like Artificial Intelligence (AI) and Machine Learning (ML). To make sure networks in today's linked digital world are safe, robust, and function well, it's crucial to embrace these cutting-edge approaches and technologies. Only then can SDN reach its full potential.

VI. References

[1] Abdi, A. H., Audah, L., Salh, A., Alhartomi, M. A., Rasheed, H., Ahmed, S., & Tahir, A. (2024). Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI and MTD Approaches to Security Solutions. *IEEE Access*.

[2] Abdulqadder, I. H., Zou, D., Aziz, I. T., Yuan, B., & Li, W. (2018). SecSDN-cloud: defeating vulnerable attacks through secure software-defined networks. *IEEE Access*, *6*, 8292-8301.

[3] Akin, E., & Korkmaz, T. (2019). Comparison of routing algorithms with static and dynamic link cost in software defined networking (SDN). IEEE Access, 7, 148629-148644.

[4] Alidadi, A., Arab, S., & Askari, T. (2022). A novel optimized routing algorithm for QoS traffic engineering in SDN-based mobile networks. ICT Express, 8(1), 130-134.

[5] Aliyu, A. L., Aneiba, A., Patwary, M., & Bull, P. (2020). A trust management framework for software defined network (SDN) controller and network applications. *Computer Networks*, *181*, 107421.

[6] Anitha, H. M., Jayarekha, P., Sivaraman, A., Mehta, A., & Nalina, V. (2024). SDN Enabled Role Based Shared Secret Scheme for Virtual Machine Security in Cloud Environment. *Cyber Security and Applications*, 100043.

[7] Cho, J. Y., & Szyrkowiec, T. (2018, August). Practical authentication and access control for software-defined networking over optical networks. In *Proceedings of the 2018 Workshop on Security in Softwarized Networks: Prospects and Challenges* (pp. 8-13).

[8] Das, D., Banerjee, S., Dasgupta, K., Chatterjee, P., Ghosh, U., & Biswas, U. (2023, January). Blockchain enabled sdn framework for security management in 5g applications. In *Proceedings of the 24th International Conference on Distributed Computing and Networking* (pp. 414-419).

[9] Golightly, L., Modesti, P., Garcia, R., & Chang, V. (2023). Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN. *Cyber Security and Applications*, 100015.

[10] Hossen, M. S., Rahman, M. H., Al-Mustanjid, M., Nobin, M. A. S., & Habib, M. A. (2019, December). Enhancing Quality of Service in SDN based on Multi-path Routing Optimization with DFS. In 2019 International Conference on Sustainable Technologies for Industry 4.0 (STI) (pp. 1-5). IEEE.

[11] Ibrahim, A. A., Hashim, F., Sali, A., Noordin, N. K., & Fadul, S. M. (2022). A multi-objective routing mechanism for energy management optimization in SDN multi-control architecture. IEEE Access, 10, 20312-20327.

[12] Iqbal, M., Iqbal, F., Mohsin, F., Rizwan, M., & Ahmad, F. (2019). Security issues in software defined networking (SDN): risks, challenges and potential solutions. *International Journal of Advanced Computer Science and Applications*, *10*(10), 298-303.

[13] Islam, M. J. (2020). Sdot-nfv: A distributed sdn based security system with iot for smart city environments. *GUB Journal of Science and Engineering (GUBJSE)*, *7*(01), 27-35.

[14] Jain, A., Jain, G., Pallavi, R., & Dadhich, A. (2023). Stacked Autoencoder Based Neural Network for Identifying Malicious Traffic in SDN. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(8s), 206-214.

[15] Jannsen, F. F. (2024). *Hierarchical temporal memory for in-car network anomaly detection* (Doctoral dissertation, Hochschule für Angewandte Wissenschaften Hamburg).

[16] Kang, H., Yegneswaran, V., Ghosh, S., Porras, P., & Shin, S. (2019). Automated permission model generation for securing SDN control-plane. *IEEE transactions on information forensics and security*, *15*, 1668-1682.

[17] Kanwal, A., Nizamuddin, M., Iqbal, W., Aman, W., Abbas, Y., & Mussiraliyeva, S. (2024). Exploring Security Dynamics in SDN Controller Architectures: Threat Landscape and Implications. *IEEE Access*.

[18] Kim, J., Seo, M., Lee, S., Nam, J., Yegneswaran, V., Porras, P., ... & Shin, S. (2024). Enhancing security in SDN: Systematizing attacks and defenses from a penetration perspective. *Computer Networks*, 110203.

[19] Mendiboure, L., Chalouf, M. A., & Krief, F. (2020, August). A scalable blockchain-based approach for authentication and access control in software defined vehicular networks. In *2020 29th International Conference on Computer Communications and Networks (ICCCN)* (pp. 1-11). IEEE.

[20] Mhamdi, L., & Isa, M. M. (2024). Securing SDN: Hybrid autoencoder-random forest for intrusion detection and attack mitigation. *Journal of Network and Computer Applications*, *225*, 103868.

[21] Midha, S., Verma, S., Mittal, M., Jhanjhi, N. Z., Masud, M., & AlZain, M. A. (2023). A Secure Multi-factor Authentication Protocol for Healthcare Services Using Cloud-based SDN. *Computers, Materials & Continua*, *74*(2).

[22] Mutaher, H., & Kumar, P. (2021). *Security-Enhanced SDN Controller Based Kerberos Authentication Protocol. 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence).* doi:10.1109/confluence51648.2021.9377044

[23] Padekar, H., Park, Y., Hu, H., & Chang, S. Y. (2016, June). Enabling dynamic access control for controller applications in software-defined networks. In *Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies* (pp. 51-61).

[24] Patwary, A. A. N., Naha, R. K., Garg, S., Battula, S. K., Patwary, M. A. K., Aghasian, E., ... & Gong, M. (2021). Towards secure fog computing: A survey on trust management, privacy, authentication, threats and access control. *Electronics*, *10*(10), 1171.

[25] Rzym, G., Masny, A., & Chołda, P. (2024). Dynamic Telemetry and Deep Neural Networks for Anomaly Detection in 6G Software-Defined Networks. *Electronics*, *13*(2), 382.

[26] Sallam, A., Refaey, A., & Shami, A. (2019). On the security of SDN: A completed secure and scalable framework using the software-defined perimeter. *IEEE access*, *7*, 146577-146587.

[27] Songa, A. V., & Karri, G. R. (2024). An integrated SDN framework for early detection of DDoS attacks in cloud computing. *Journal of Cloud Computing*, *13*(1), 64.

[28] Yue, M., Wang, H., Liu, L., & Wu, Z. (2020). Detecting DoS attacks based on multi-features in SDN. IEEE Access, 8, 104688-104700.
[29] Dridi, L., & Zhani, M. F. (2018). A holistic approach to mitigating DoS attacks in SDN networks. International Journal of Network Management, 28(1), e1996.
[30] Goksel, N., & Demirci, M. (2019, June). DoS attack detection using packet statistics in SDN. In 2019 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1-6). IEEE.