SD-WAN ARCHITECTURAL MODELS: A LITERATURE REVIEW OF CENTRALIZED, DISTRIBUTED, AND HYBRID CONTROL PLANE DESIGNS

Wahyudi

Faculty of Informatic Computer and Technology Universitas Horizon Indonesia
Jl. Pangkal Perjuangan By Pass No.KM.1, Tanjungpura, Kec. Karawang Bar.,
Karawang, Jawa Barat 41316

Email: wahyudi.wahyudi.krw@horizon.ac.id

ABSTRACT

Software-Defined Wide Area Networking (SD-WAN) has emerged as a transformative solution for modern network management, offering agility, cost-efficiency, and enhanced security over traditional WAN architectures. This paper presents a systematic literature review of SD-WAN control plane designs, categorizing them into centralized, distributed, and hybrid models. The centralized approach, governed by a single controller, simplifies policy enforcement but introduces scalability bottlenecks and single-point-of-failure risks. Distributed architectures mitigate these issues by decentralizing control, improving resilience at the cost of synchronization complexity. Hybrid models strike a balance, combining global policy coordination with localized decision-making. Through a rigorous methodology—encompassing keyword-based searches, inclusion/exclusion criteria, and thematic synthesis—we analyze 1) the trade-offs between these architectures, 2) their performance under scalability and security threats (e.g., DDoS attacks, controller compromises), and 3) emerging mitigation strategies (e.g., clustering, zero-trust frameworks). Key findings reveal that while centralized designs dominate enterprise deployments, hybrid models are gaining traction for multi-cloud environments. The review also identifies gaps in standardized security protocols and AI-driven dynamic control plane adaptation, suggesting future research directions. This work provides a foundational reference for network architects and researchers evaluating SD-WAN design paradigms.

Keywords: Software Defined Wide Area Networking, Architectural Models, Security Threads

1. INTRODUCTION

Software-Defined Wide Area Networking has emerged as a transformative technology, revolutionizing how organizations manage and optimize their wide area networks [2]. Traditional IP networks, despite their ubiquity, often grapple with inherent complexities that impede efficient management and adaptability [3]. SD-WAN addresses these challenges by decoupling the control plane from the data plane, introducing a centralized controller that orchestrates network behavior [4], [5]. This innovative approach empowers network administrators with the ability to program, control, and manage network components, fostering greater agility, visibility, and cost-effectiveness [6]. SD-WAN's core strength lies in its capability to abstract the underlying network infrastructure, presenting a unified, logical view that simplifies network management tasks [7]. As a result, enterprises can dynamically adjust network configurations to meet changing business needs, optimize application performance, and enhance security posture. The genesis of Software-Defined Networking can be traced back to the idea of separating the forwarding or data plane from the control plane, allowing programmability within the control plane [8].

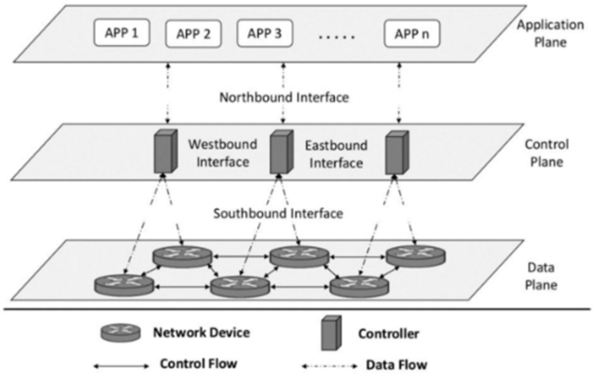

Figure 1. . Software Defined Networking (SDN) General Architecture [1]

The separation of the control plane from individual network devices, coupled with its implementation in an external software entity, marks a significant departure from conventional networks [9]. This architectural shift enables the centralization of network intelligence, fostering enhanced network control and automation [10]. The centralized control plane, often implemented as a software controller, acts as the brain of the network, dictating how data packets are forwarded across the network infrastructure. This approach facilitates the implementation of sophisticated traffic engineering policies, quality of service guarantees, and security measures. As SDN gained traction, its architectural principles were extended to the wide area network, giving rise to SD-WAN. SD-WAN is conceptually rooted in software-defined networking principles [11].

The advantages of SD-WAN system from its centralized control, which enables efficient resource utilization and improved network performance [12]. The centralized control element in SDN acts as the network's central command center, making it easier to implement policies across the whole infrastructure [13] [14]. SD-WAN solutions have rapidly gained prominence, offering enterprises a compelling alternative to traditional WAN architectures. The increasing adoption of cloud-based applications and services, coupled with the demand for improved application performance and enhanced security, has fueled the growth of the SD-WAN market. SD-WAN's adaptability, cost-effectiveness, and enhanced security capabilities have positioned it as a strategic enabler for digital transformation.

1.1. SD-WAN Control Plane Architectures

SD-WAN architectures can be broadly classified into three primary categories based on their control plane design: centralized, distributed, and hybrid. In the **centralized** control plane architecture, a single, logically centralized controller manages the entire network. This controller possesses a global view of the network topology, traffic conditions, and application requirements. The controller has complete knowledge of the network, enabling it to make informed decisions regarding traffic routing, policy enforcement, and resource allocation. This approach simplifies network management, enabling administrators to configure and monitor the network from a single point of control. The controller centrally manages network policies, security measures, and traffic engineering rules [13].

However, the centralized architecture also presents potential limitations. The central controller acts as a single point of failure. The failure of the controller can disrupt network operations, potentially leading to service outages. Another concern is scalability; as the network grows, the controller may become a bottleneck, struggling to handle the increasing volume of control plane traffic and network state information. The centralized architecture is vulnerable to disruptions and attacks, especially those targeting single points of failure [15], [16]. Furthermore, the centralized architecture can introduce latency, as all control plane communications must traverse the central controller.

The distributed control plane architecture addresses some of the limitations of the centralized approach by distributing control plane functions across multiple controllers or network devices. Each controller manages a specific domain or region of the network. The controller shares information with other controllers to maintain a consistent view of the network. This approach enhances scalability and resilience, as the failure of one controller does not necessarily disrupt the entire network. The distributed control plane offers enhanced scalability, as the control plane workload is distributed across multiple controllers.

However, the distributed architecture also introduces complexities. Maintaining consistency across multiple controllers can be challenging, requiring sophisticated synchronization mechanisms. Implementing distributed control can lead to increased network management complexity, as administrators must manage multiple controllers and ensure their consistent operation. Moreover, the distributed architecture may require more sophisticated security measures to protect against attacks targeting individual controllers [17].

The hybrid control plane architecture combines elements of both centralized and distributed approaches. In a hybrid approach, a central controller may be responsible for high-level policy management and network-wide coordination, while distributed controllers handle local control plane functions. This architecture aims to leverage the strengths of both approaches, providing a balance between centralized control and distributed autonomy. A hybrid control plane can offer a good compromise between centralized control and distributed autonomy.

1.2. Centralized Control Plane Designs

The centralized control plane design in SD-WAN architectures revolves around a single, logically centralized controller that oversees and manages the entire network [18]. This controller acts as the central decision-making entity, responsible for routing, policy enforcement, and resource allocation [19]. The controller maintains a global view of the network topology, traffic conditions, and application requirements, enabling it to make informed decisions that optimize network performance and efficiency. The centralized control plane offers several advantages, including simplified network management, consistent policy enforcement, and enhanced visibility. Centralized control simplifies network management by providing a single point of control for configuration, monitoring, and troubleshooting [20]. Administrators can manage the entire network from a single interface, reducing the complexity of network operations. A centralized controller can ensure consistent policy enforcement across the entire network, regardless of the location of the user or application [12].

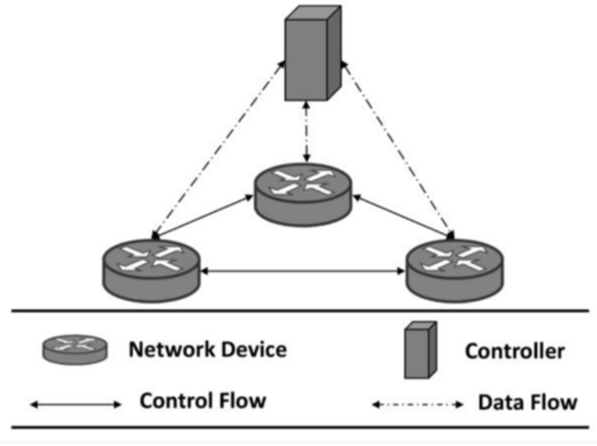

Figure 2. Centralized Control Plane Designs [1].

However, the centralized control plane also presents several challenges. Scalability is a major concern, as the central controller can become a bottleneck as the network grows [21].

The controller may struggle to handle the increasing volume of control plane traffic and network state information, leading to performance degradation. A centralized architecture is vulnerable to distributed denial-of-service attacks [22]. The failure of the central controller can disrupt network operations, potentially leading to service outages. The failure of one can cause massive disruption in operations.

To address these challenges, various techniques have been developed to enhance the scalability and resilience of centralized control plane designs. Techniques like clustering and hierarchical control can be used to scale the performance of centralized systems. Clustering involves deploying multiple controllers in a cluster, where each controller shares the control plane workload [14].

Hierarchical control involves dividing the network into multiple domains, each managed by a local controller, with a central controller providing overall coordination.

1.3. Distributed Control Plane Designs

Distributed control plane designs in SD-WAN architectures aim to overcome the limitations of centralized approaches by distributing control plane functions across multiple controllers or network devices [11]. Each controller manages a specific domain or region of the network and collaborates with other controllers to maintain a consistent view of the overall network state.

This distribution of control plane responsibilities enhances scalability and resilience, as the failure of one controller does not necessarily disrupt the entire network. The distribution also reduces the risk of congestion at a central control point. Distributed control planes offer enhanced scalability, as the control plane workload is distributed across multiple controllers. The distribution of controllers allows the network to scale more easily to accommodate growing bandwidth demands.

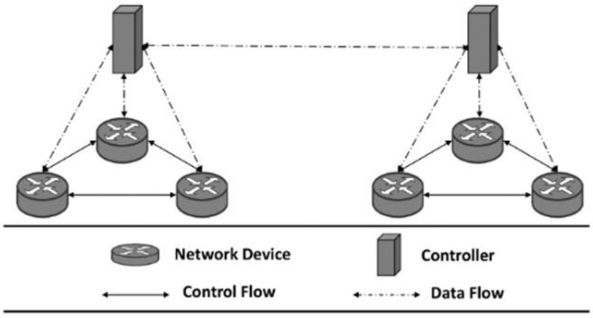

Figure 3. Distributed Flat Controllers Design [1].

However, distributed control plane designs also introduce complexities. Maintaining consistency across multiple controllers can be challenging, requiring sophisticated synchronization mechanisms. Moreover, the distributed architecture may require more sophisticated security measures to protect against attacks targeting individual controllers.

The need for a hybrid SDN approach in network management arises from the limitations of traditional distributed systems and the vulnerabilities inherent in centralized control [14]. This is addressed by decoupling the data and control planes within network equipment and employing a centralized controller for comprehensive network oversight [23], [24].

SDN provides complete programmability that allows for optimal load-balancing [25]. Also, it provides more control over the packets in the network. This flexibility can be leveraged to address the limitations of traditional distributed systems and the vulnerabilities inherent in centralized control [26].

1.4. Hybrid Control Plane Designs

Hybrid control plane architectures in SD-WAN combine elements of both centralized and distributed approaches, aiming to leverage the strengths of each while mitigating their weaknesses.

In a hybrid model, a central controller may be responsible for high-level policy management, network-wide coordination, and global optimization, while distributed controllers handle local control plane functions, such as routing within a specific domain or enforcing policies at the edge of the network.

This architecture aims to provide a balance between centralized control and distributed autonomy, enabling efficient network management, scalability, and resilience [26].

A hybrid control plane allows for flexible allocation of control plane responsibilities, adapting to the specific needs of the network. The ability to customize control plane responsibilities is advantageous in cloud computing due to the sensitivity and the need to manage security effectively [28].

Hybrid control planes offer a number of advantages. The central controller provides a unified view of the network and facilitates consistent policy enforcement, while the distributed controllers ensure scalability and resilience.

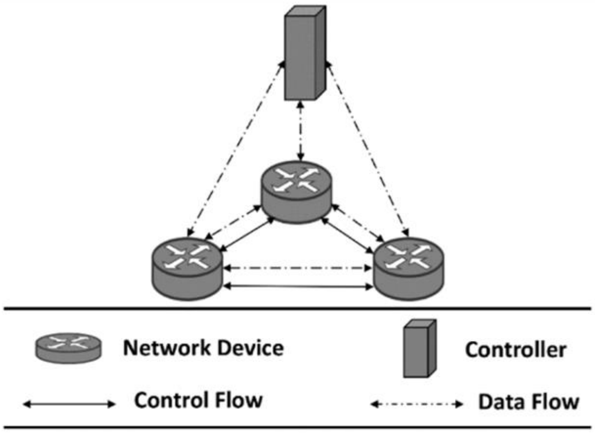

Figure 4. Hybrid Control Plane Designs [1].

However, hybrid control plane designs can be complex to implement and manage, requiring careful coordination between the central and distributed components. SDN leverages network programmability, open interfaces, centralized management, and abstraction to improve performance parameters, enabling agility and flexibility [29].

Security Considerations in SD-WAN Architectures

Security is a critical consideration in SD-WAN architectures, regardless of the control plane design [30], [31]. Centralized control planes offer a single point of control for security policy enforcement, but also represent a single point of failure [32].

The centralized nature of SDN, while offering advantages in management and control, introduces vulnerabilities that can be exploited to disrupt network operations, compromise sensitive data, and launch attacks [33].

Distributed control planes enhance resilience by distributing the risk across multiple controllers, but also require robust security mechanisms to protect against attacks targeting individual controllers. In general, SDN security solutions can be categorized into those that utilize built-in features of SDN and those that provide external SDN applications that run above the controller [34]. Hybrid control planes require a combination of security measures to protect both the central controller and the distributed components.

Several security threats are relevant to the different architectural models. For centralized control planes, Distributed Denial-of-Service attacks targeting the central controller can disrupt the entire network [35]. Compromise of the central controller can lead to widespread policy violations. For distributed control planes, vulnerabilities in individual controllers can be exploited to gain control over specific network domains. Lack of consistency across controllers can lead to security policy inconsistencies.

For hybrid control planes, attacks targeting the central controller can disrupt network-wide policy management. Compromise of distributed controllers can lead to localized security breaches. To mitigate these threats, a number of security measures can be implemented [36].

These measures include:

- Strong authentication and authorization mechanisms to protect access to the control plane [37].
- Intrusion detection and prevention systems to detect and block malicious traffic.
- Security policies that are well defined and consistently enforced across the network.
- Regular security audits to identify and address vulnerabilities.

Research has been done on the security vulnerabilities of SDN, possible attacks and solutions to protect it [30]. Security should be a primary consideration in the design and deployment of SD-WAN architectures.

1. METHOD

The systematic literature review methodology will be employed to synthesize existing research on SD-WAN architectural models, focusing on centralized, distributed, and hybrid control plane designs. The approach will involve a structured process for identifying, selecting, evaluating, and synthesizing relevant studies to provide a comprehensive overview of the topic. For a paper to be included in the review, it must meet certain criteria [38].

The review process will consist of several key steps.

- First, a comprehensive search strategy will be developed to identify relevant studies from academic databases, industry reports, and other sources, which will be based on keywords and search strings related to SD-WAN, control plane architectures, centralized control, distributed control, and hybrid control.
- Second, the identified studies will be screened based on predefined inclusion and exclusion criteria to ensure that only relevant and high-quality studies are included in the review, such as studies focusing on SD-WAN architectures, control plane designs, security considerations, and performance evaluations.
- Third, data will be extracted from the included studies using a standardized data extraction form to capture relevant information such as study design, sample size, intervention, outcome measures, and key findings.

To minimize biases, errors, and misinterpretations in the review process, consistency in the presentation of ideas, originality to avoid duplication, and a rigorous methodological approach will be considered.
The screening and selection of articles are conducted by the two researchers themselves. The selected articles are the ones that contribute to answering the research

questions, namely the success factors of the digital transformation of SMEs.

2. RESULT AND DISCUSSION

The results of the systematic literature review will be presented in a structured manner, summarizing the key findings from the included studies. The review should identify the primary SD-WAN architectural models, analyze the advantages and disadvantages of each model, and assess the performance, scalability, and security characteristics of each model, revealing the state of research on digital transformation [39].

The findings will be synthesized to identify common themes, patterns, and gaps in the existing literature, providing insights into the current state of research and potential areas for future investigation [40]. It is important to review titles and abstracts to exclude irrelevant studies [41]. This step is crucial in narrowing down the vast number of potential studies to those most relevant to the research questions [41]. This organized approach aids in systematically analyzing the latest developments in the field [42]. The extracted data will be synthesized, focusing on key themes such as challenges, opportunities, and regional differences, ensuring that all relevant information is captured [41].

The findings will be synthesized to identify common themes, patterns, and gaps in the existing literature, providing insights into the current state of research and potential areas for future investigation [40]. It is important to review titles and abstracts to exclude irrelevant studies [41]. This step is crucial in narrowing down the vast number of potential studies to those most relevant to the research questions [41]. This organized approach aids in systematically analyzing the latest developments in the field [42]. The extracted data will be synthesized, focusing on key themes such as challenges, opportunities, and regional differences, ensuring that all relevant information is captured [41].

4. CONCLUSION

The systematic literature review undertaken in this study provides a comprehensive synthesis of existing research on SD-WAN architectural models, specifically focusing on centralized, distributed, and hybrid control plane designs. The review identified the key characteristics, advantages, and disadvantages of each architectural model, highlighting their suitability for different network environments and application requirements. . The analysis of performance, scalability, and security considerations further elucidated the trade-offs associated with each design choice, offering valuable insights for network architects and decision-makers. [43]. By consolidating the findings from various studies, this review offers a holistic perspective on the current state of SD-WAN technology and its potential for future development. [44]. It also underscores the necessity for SMEs to adopt digital technologies to remain competitive in the modern business landscape, as well as the importance of tailored strategies that account for regional differences in infrastructure, skills, and regulatory environments [41].

References

[1] Abuarqoub, A. A Review of the Control Plane Scalability Approaches in Software Defined Networking. *Future Internet* **2020**, *12*, 49. https://doi.org/10.3390/fi12030049

[2] A Abdou, P. C. van Oorschot, and T. Wan, “Comparative Analysis of Control Plane Security of SDN and Conventional Networks,” IEEE Communications Surveys & Tutorials, vol. 20, no. 4, p. 3542, Jan. 2018, doi: 10.1109/comst.2018.2839348.

[3] D. Kreutz, F. M. V. Ramos, P. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-Defined Networking: A Comprehensive Survey,” arXiv (Cornell University), Jan. 2014, doi: 10.48550/arxiv.1406.0440.

[4] M. Borokhovich and S. Schmid, “How (Not) to Shoot in Your Foot with SDN Local Fast Failover: A Load-Connectivity Tradeoff,” arXiv (Cornell University), Jan. 2013, doi: 10.48550/arxiv.1309.3150.

[5] L. Wang, A. F. Anta, F. Zhang, J. Wu, and Z. Liu, “Multi-resource

Energy-efficient Routing in Cloud Data Centers with Networks-as-a-Service," arXiv (Cornell University), Jan. 2015, doi: 10.48550/arxiv.1501.05086.

[6] K. Alwasel et al., "IoTSim-SDWAN: A simulation framework for interconnecting distributed datacenters over Software-Defined Wide Area Network (SD-WAN)," Journal of Parallel and Distributed Computing, vol. 143, p. 17, May 2020, doi: 10.1016/j.jpdc.2020.04.006.

[7] C. J. ́e M. Diaz, L. Andrade–Arenas, J. G. U. Arellano, and M. Á. C. Lengua, "Analysis about Benefits of Software-Defined Wide Area Network: A New Alternative for WAN Connectivity," International Journal of Advanced Computer Science and Applications, vol. 13, no. 1, Jan. 2022, doi: 10.14569/ijacsa.2022.0130188.

[8] M. Jammal, T. Singh, A. Shami, R. Asal, and Y. Li, "Software-Defined Networking: State of the Art and Research Challenges," arXiv (Cornell University), Jan. 2014, doi: 10.48550/arxiv.1406.0124.

[9] T. Wan, A. Abdou, and P. C. van Oorschot, "A Framework and Comparative Analysis of Control Plane Security of SDN and Conventional Networks," arXiv (Cornell University), Jan. 2017, doi: 10.48550/arxiv.1703.06992.

[10] C. Zhao and F. Liu, "DDoS Attack Detection Based on Self-organizing Mapping Network in Software Defined Networking," MATEC Web of Conferences, vol. 176, p. 1026, Jan. 2018, doi: 10.1051/matecconf/201817601026.

[11] K. Kirkpatrick, "Software-defined networking," Communications of the ACM, vol. 56, no. 9, p. 16, Aug. 2013, doi: 10.1145/2500468.2500473.

[12] R. Swami, M. Dave, and V. Ranga, "Software-defined Networking-based DDoS Defense Mechanisms," ACM Computing Surveys, vol. 52, no. 2. Association for Computing Machinery, p. 1, Apr. 09, 2019. doi: 10.1145/3301614.

[13] S. Saraswat, V. Agarwal, H. P. Gupta, R. Mishra, A. Gupta, and T. Dutta, "Challenges and solutions in Software Defined Networking: A survey," Journal of Network and Computer Applications, vol. 141, p. 23, May 2019, doi: 10.1016/j.jnca.2019.04.020.

[14] M. Osman and J. Mangues-Bafalluy, "Hybrid SDN Performance: Switching between Centralized and Distributed Modes under Unreliable Control Communication Channels," Journal of Sensor and Actuator Networks, vol. 10, no. 3, p. 57, Aug. 2021, doi: 10.3390/jsan10030057.

[15] S. Wang, K. Gomez, S. Kandeepan, M. R. Asghar, G. Russello, and P. Zanna, "Mitigating DDoS Attacks in SDN-Based IoT Networks Leveraging Secure Control and Data Plane Algorithm," Applied Sciences, vol. 11, no. 3, p. 929, Jan. 2021, doi: 10.3390/app11030929.

[16] S. S. Savas, M. Tornatore, M. F. Habib, P. Chowdhury, and B. Mukherjee, "Disaster-Resilient Control Plane Design and Mapping in Software-Defined Networks," arXiv (Cornell University), Jan. 2015, doi: 10.48550/arxiv.1509.00509.

[17] B. Karim, S. Hameed, and G. Muhammad, "A Centralized Reputation Management Scheme for Isolating Malicious Controller(s) in Distributed Software-Defined Networks," International Journal of Advanced Computer Science and Applications, vol. 7, no. 12, Jan. 2016, doi: 10.14569/ijacsa.2016.071248.

[18] Z. Allybokus, K. Avrachenkov, J. Leguay, and L. Maggi, "Real-Time Fair Resource Allocation in Distributed Software Defined Networks," vol. 3, p. 19, Sep. 2017, doi: 10.23919/itc.2017.8064335.

[19] S. Faizullah and S. Almutairi, "Vulnerabilities in SDN Due to Separation of Data and Control Planes," International Journal of Computer Applications, vol. 179, no. 31, p. 21, Apr. 2018, doi: 10.5120/ijca2018916519.

[20] S. Chattopadhyaya and A. K. Sahoo, "Software defined networks: Current problems and future solutions," Materials Today Proceedings, vol. 49,

p. 2989, Nov. 2020, doi: 10.1016/j.matpr.2020.09.568.

[21] Z. Zhang, L. Ma, K. K. Leung, F. Le, S. Kompella, and L. Tassiulas, "How Better is Distributed SDN? An Analytical Approach," arXiv (Cornell University), Jan. 2017, doi: 10.48550/arxiv.1712.04161.

[22] A. Hamarshe, H. I. Ashqar, and M. M. N. Hamarsheh, "Detection of DDoS Attacks in Software Defined Networking Using Machine Learning Models," in Lecture notes in networks and systems, Springer International Publishing, 2023, p. 640. doi: 10.1007/978-3-031-33743-7_51.

[23] U. N. Kadim and I. J. Mohammed, "SDN-RA: An Optimized Reschedule Algorithm of SDN Load Balancer for Data Center Networks Based on QoS," in IOP Conference Series Materials Science and Engineering, IOP Publishing, Nov. 2020, p. 32057. doi: 10.1088/1757-899x/928/3/032057.

[24] C. DeCusatis, "Reference Architecture for Multi-Layer Software Defined Optical Data Center Networks," Electronics, vol. 4, no. 3, p. 633, Sep. 2015, doi: 10.3390/electronics4030633.

[25] M. Caria and A. Jukan, "Link Capacity Planning for Fault Tolerant Operation in Hybrid SDN/OSPF Networks," arXiv (Cornell University), Jan. 2016, doi: 10.48550/arxiv.1604.05534.

[26] D. N. Pratiwi, M. Faiqurahman, and D. R. Akbi, "Analisis Distance Vector Protocol Routing dan Link State Routing Protocol Pada Jaringan Software Defined Network," Jurnal Repositor, vol. 2, no. 3, Jan. 2024, doi: 10.22219/repositor.v2i3.30502.

[27] A. Hakiri, A. Gokhale, P. Berthou, D. C. Schmidt, and T. Gayraud, "Software-Defined Networking: Challenges and research opportunities for Future Internet," Computer Networks, vol. 75, p. 453, Oct. 2014, doi: 10.1016/j.comnet.2014.10.015.

[28] A. Rahman et al., "Enhancing Data Security for Cloud Computing Applications through Distributed Blockchain-based SDN Architecture in IoT Networks," arXiv (Cornell University), Jan. 2022, doi: 10.48550/arxiv.2211.15013.

[29] S. Abdollahi, A. Deldari, H. Asadi, A. Montazerolghaem, and S. M. Mazinani, "Flow-Aware Forwarding in SDN Datacenters Using a Knapsack-PSO-Based Solution," IEEE Transactions on Network and Service Management, vol. 18, no. 3, p. 2902, Mar. 2021, doi: 10.1109/tnsm.2021.3064974.

[30] J. P. Mabel, V. Reddy, and K. N. Babu, "SDN Security: Challenges and Solutions," in Lecture notes in electrical engineering, Springer Science+Business Media, 2019, p. 837. doi: 10.1007/978-981-13-5802-9_73.

[31] K. Gaur, P. Choudhary, P. Yadav, A. Jain, and P. Kumar, "Software Defined Networking: A review on Architecture, Security and Applications," IOP Conference Series Materials Science and Engineering, vol. 1099, no. 1. IOP Publishing, p. 12073, Mar. 01, 2021. doi: 10.1088/1757-899x/1099/1/012073.

[32] J. Spooner and D. Shao, "A Review of Solutions for SDN-Exclusive Security Issues," International Journal of Advanced Computer Science and Applications, vol. 7, no. 8. Science and Information Organization, Jan. 01, 2016. doi: 10.14569/ijacsa.2016.070817.

[33] G. Logeswari, S. K. Bose, and T. Anitha, "An Intrusion Detection System for SDN Using Machine Learning," Intelligent Automation & Soft Computing, vol. 35, no. 1, p. 867, Jun. 2022, doi: 10.32604/iasc.2023.026769.

[34] A. M. Abdelrahman et al., "Software-defined networking security for private data center networks and clouds: Vulnerabilities, attacks, countermeasures, and solutions," International Journal of Communication Systems, vol. 34, no. 4, Dec. 2020, doi: 10.1002/dac.4706.

[35] J. Singh and S. Behal, "Detection and mitigation of DDoS attacks in SDN: A comprehensive

review, research challenges and future directions," Computer Science Review, vol. 37, p. 100279, Jun. 2020, doi: 10.1016/j.cosrev.2020.100279.

[36] M. Iqbal, F. Iqbal, F. Mohsin, M. Rizwan, and F. Ahmad, "Security Issues in Software Defined Networking (SDN): Risks, Challenges and Potential Solutions," International Journal of Advanced Computer Science and Applications, vol. 10, no. 10, Jan. 2019, doi: 10.14569/ijacsa.2019.0101042.

[37] Y. Tseng, F. Naït-Abdesselam, and A. Khokhar, "A comprehensive 3-dimensional security analysis of a controller in software-defined networking," Security and Privacy, vol. 1, no. 2, Mar. 2018, doi: 10.1002/spy2.21.

[38] S. Peltomaa Åström and S. Winoy, "Automating Software Development Processes Through Multi-Agent Systems." May 30, 2024.

[39] S. Lokuge and S. X. Duan, "Towards Understanding Enablers of Digital Transformation in Small and Medium-Sized Enterprises," arXiv (Cornell University), Jan. 2021, doi: 10.48550/arxiv.2111.05989.

[40] T. V. Iyelolu, E. E. Agu, C. Idemudia, and T. I. Ijomah, "Driving SME innovation with AI solutions: overcoming adoption barriers and future growth opportunities," International Journal of Science and Technology Research Archive, vol. 7, no. 1, p. 36, Aug. 2024, doi: 10.53771/ijstra.2024.7.1.0055.

[41] S. O. Yusuf, R. L. Durodola, G. Ocran, J. E. Abubakar, A. Z. Echere, and A. H. Paul-Adeleye, "Challenges and opportunities in AI and digital transformation for SMEs: A cross-continental perspective." Mar. 2024.

[42] L. Zou, L. Wan, H. Wu, J. Liu, and P. Gao, "Measuring Corporate Digital Transformation: Methodology, Indicators and Applications," Sustainability, vol. 16, no. 10, p. 4087, May 2024, doi: 10.3390/su16104087.

[43] J. Reis and N. Mel□ão, "Digital transformation: A meta-review and guidelines for future research," Heliyon, vol. 9, no. 1. Elsevier BV, Jan. 01, 2023. doi: 10.1016/j.heliyon.2023.e12834.

[44] R. Aleid and F. Almisned, "Analysis of the impact of technological advances and new trends on Digital Transformation strategies," Proceedings of the World Congress on Electrical Engineering and Computer Systems and Science, Aug. 2024, doi: 10.11159/cist24.148.