CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES

https://cajmtcs.casjournal.org/index.php/CAJMTCS

*Volume: 03 Issue: 07 | July 2022 ISSN: 2660-5309*

*Article*

# Evolution of Software-Defined Networking in Enterprise and Service Provider Networks: Opportunities, Challenges, and Future Directions

**Afsara Tasnim Shama**

1. Department of Computer Science, Independent University, Bangladesh

*Correspondence : tasnimafsara20@gmail.com

**Abstract:** Background: The fast growth of cloud computing, virtualization, artificial intelligence, and digital transformation have made networking systems in enterprises and service providers more complicated, thus raising the need for intelligent, flexible, and scalable network management solutions. Software-defined networking is an innovative approach in networking that enhances centralized control, automation, efficiency of resource usage, and service provision. Methods: A quantitative study employing a cross-sectional online survey was undertaken with 175 network professionals across the United States. Data collection was done through an online questionnaire while IBM SPSS Statistics 29 was used for data analysis. Descriptive statistics, Pearson correlation test, and multiple regression were some of the methods applied. Results: It was found that 43.4% of firms have implemented software-defined networking. Network agility (89.1%) was recognized as the greatest organizational benefit, while the legacy infrastructure integration (25.7%) served as the greatest implementation issue. Pearson correlation test showed that there were significant positive correlations between all research variables. Multiple regression analysis proved that software-defined networking had the greatest positive impact on the network performance ($\beta = 0.298$, $p < 0.001$) and the developed model could explain 73.4% of the network performance variance ($R^2 = 0.734$). In addition, all formulated hypotheses were supported statistically. Conclusion: Software-defined networking considerably improves the network performance in an organization through the improvement of automation, scalability, traffic optimization, and centralization. Although some implementation issues exist, companies implementing integrated software-defined networking systems are capable of creating secure and resilient network infrastructures ready for future sustainable digital transformation.

**Keywords:** Network Automation, Network Performance, Software-Defined Networking, Service Provider Networks, Enterprise Networks

**Citation:** Shama, A. T. Evolution of Software-Defined Networking in Enterprise and Service Provider Networks: Opportunities, Challenges, and Future Directions. Central Asian Journal of Mathematical Theory and Computer Sciences 2022, 3(7), 75-83

Received: 10th Apr 2022
Revised: 29th May 2022
Accepted: 18th June 2022
Published: 25th July 2022



## 1. Introduction

Digital transformation has brought about changes in the way modern-day communication networks are structured and managed [1]. Technological advancements in cloud computing, edge computing, artificial intelligence, 5G technology, and the Internet of Things have led to an unprecedented level of network traffic as well as increased expectations with regard to network performance [2]. There is a need for enterprise companies and service providers to deliver highly performant networks that can effectively cope with dynamic loads and distributed applications [3]. But traditional network infrastructures, based on hardware-driven systems and manually-configured components, do not possess the agility and programmability needed to meet these demands. In the growing world of digital ecosystems, there is a need for more intelligent networks to ease the process of network management [4], [5].

Software-defined networking has been revealed to be one of the most important innovations that have taken place in modern network architecture as a result of changes in how communication networks can be created, managed, and optimized [6]. Software-defined networking is quite different from traditional networking in that it ensures separation of intelligence from forwarding devices in order to achieve centralization of control, configuration, and programmability of the resources used throughout the whole network infrastructure [7]. In doing so, software-defined networking makes it easier and faster to deploy network services, optimize traffic flows, utilize bandwidth, enhance security policies, and minimize complexity of operations [8].

Despite all the strengths, a smooth execution process is not an easy task for many companies. Integration of SDN into the current infrastructure needs special knowledge, significant investment and organizational readiness [9]. Issues related to the availability of the controller, compatibility of multivendor systems, cybersecurity, complexity of the migration process, as well as regulatory issues, still play a role in the decision-making process [10]. Moreover, the development and increasing use of such technologies as artificial intelligence, edge intelligence, and mission-critical applications have set up new performance requirements for the network [11].

While there is no lack of scholarly work on network architecture, virtualization technology, routing optimizations, and controllers design, there is noticeably less empirical study of the organizational aspects of adoption of software-defined networking based on the perspectives of industry experts [12]. The majority of existing literature focuses on technological aspects and provides little information about the effect of automation, traffic optimization, security and policy management, and network scalability as a whole on the organizational performance. Thus, this study is focused on the analysis of the development of software-defined networking in corporate and service provider networks based on an online quantitative survey of 175 networking professionals in the USA. This study analyses the effects of software-defined networking adoption, network automation, traffic optimization, security and policy management, and scalability and flexibility on network performance.

## 2. Materials and Methods

### 2.1 Research Design and Data Collection

This research made use of a quantitative cross-sectional survey design for the examination of the development of Software-Defined Networking (SDN) in enterprise and service providers' networks within the USA. An online survey was designed on the basis of a thorough literature review on the following concepts related to SDN: network virtualization, cloud networking, and software-defined infrastructure. The survey questions were created to analyze the impact of SDN adoption, network automation, traffic optimization, security and policy control, and scalability and flexibility on the overall network performance [13], [14]. The survey data were collected from January to March 2022 by Google Forms, while the survey link was posted on professional networking websites such as LinkedIn, technological forums, enterprise IT community websites, and industry mailing lists. The total number of responses received was 196; however, only 175 completed surveys were considered for analysis, which gave an effective response rate of 89.3%.

### 2.2 Measurement of Variables

The survey comprised of two parts. The first part asked for demographic data on gender, age, educational qualification, organizational affiliation, and experience level. The second part sought to measure six research constructs through a series of multiple items based on established research in networking, cloud computing, and information systems studies. SDNA, NA, TO, SPC, and SF were used as independent variables, whereas NP was used as a dependent variable. Each measurement item was rated on a five-point Likert scale, which started from "1=Strongly Disagree" to "5=Strongly Agree" [15]. Prior to distribution, the questionnaire was piloted among networking professionals in order to enhance the validity of the measurement items [16].

2.3 Statistical Analysis

Analysis of the data was conducted using IBM SPSS Statistics version 29. Descriptive statistics such as frequency distribution, percentages, means, and standard deviations were applied in order to provide summary statistics for demographic profile of the participants and their response towards study variables [17]. Pearson correlation analysis was done to identify the relationship between study constructs, and multiple linear regression analysis was done to identify the effect of independent variables on network performance [18]. Model adequacy was evaluated by R squared, Adjusted R squared, F-statistic, and Durbin Watson statistic; while multicollinearity was tested using Variance Inflation Factor (VIF). The level of statistical significance was set at 95 percent [19].

2.4 Research Framework

The theoretical framework suggested herein makes an assumption that the effective implementation of SDN will positively affect the performance of organizational networks by increasing their automation, traffic optimization, centralized security, and scalability capabilities [20]. Therefore, five hypotheses were stated to assess the impact of SDNA, NA, TO, SPC, and SF on Network Performance directly. This theoretical framework helps analyze the contribution made by SDN technology to operational efficiency and digital transformation and provides insights into future perspectives in software-defined networking [21].

## 3. Results

3.1 Demographic Characteristics of Respondents

**Table 1.** Demographic Characteristics of Respondents

| Variable | Category | Frequency (n) | Percentage (%) |
|---|---|---|---|
| Gender | Male | 114 | 65.1 |
| | Female | 57 | 32.6 |
| | Prefer not to say | 4 | 2.3 |
| Age (Years) | 25–34 | 39 | 22.3 |
| | 35–44 | 61 | 34.9 |
| | 45–54 | 48 | 27.4 |
| | ≥55 | 27 | 15.4 |
| Education | Bachelor's | 42 | 24.0 |
| | Master's | 82 | 46.9 |
| | Doctorate | 36 | 20.6 |
| | Professional Certification | 15 | 8.5 |
| Organization Type | Enterprise | 95 | 54.3 |
| | Service Provider | 58 | 33.1 |
| | Cloud Provider | 22 | 12.6 |
| Experience | 1–5 Years | 27 | 15.4 |
| | 6–10 Years | 49 | 28.0 |
| | 11–15 Years | 54 | 30.9 |
| | >15 Years | 45 | 25.7 |

The demographic profile of the 175 survey participants demonstrates a diverse and highly experienced sample of professionals in the area of networking as shown in **Table 1.** There were more male (65.1%) than female participants (32.6%) with only 2.3% not willing to disclose their gender details. Respondents in the age category of 35-44 years made the highest percentage of (34.9%) while those in the age category of 45-54 years made 27.4%. This means that many participants had been in their careers and thus have much experience. As shown in Table 1, there were 46.9% who had master's degree while

24.0% had bachelor's degrees, 20.6% had doctoral degrees, and 8.5% had professional certifications. Additionally, from Table 1 above, it can be seen that 54.3% of participants worked in enterprises while 33.1% were employed in service providers and 12.6% in cloud providers. Finally, the most number of participants (30.9%) had an experience of 11-15 years while 28.0% had an experience of 6-10 years.

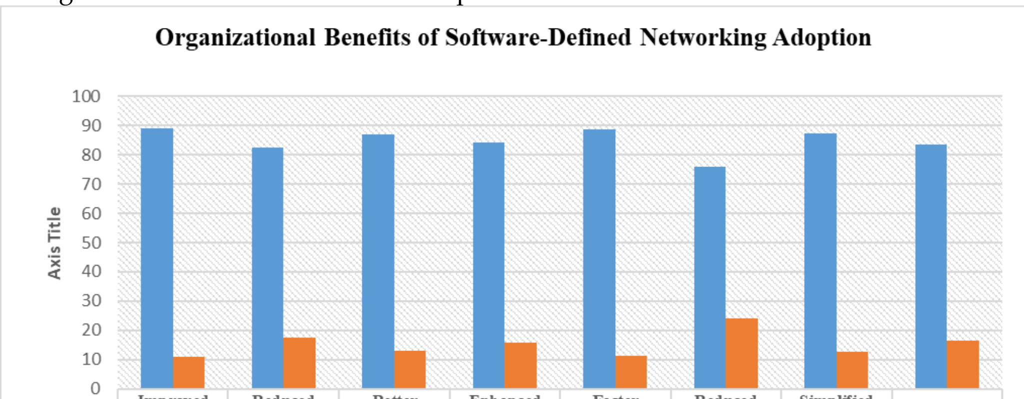
### 3.2 Software-Defined Networking Adoption Characteristics

**Table 2.** Software-Defined Networking Adoption Characteristics

| Variable | Category | Frequency | Percentage (%) |
|---|---|---|---|
| SDN Deployment Status | Fully Implemented | 76 | 43.4 |
| | Partially Implemented | 71 | 40.6 |
| | Pilot Stage | 28 | 16.0 |
| SDN Controller | Cisco ACI | 58 | 33.1 |
| | VMware NSX | 41 | 23.4 |
| | Open Day light | 33 | 18.9 |
| | Juniper Contrail | 22 | 12.6 |
| | Others | 21 | 12.0 |
| Primary Network Type | Enterprise LAN | 82 | 46.9 |
| | Data Center | 47 | 26.9 |
| | WAN | 28 | 16.0 |
| | Hybrid Cloud | 18 | 10.2 |

The adoption factors for the sampled organizations adopting the SDN technology are presented in **Table 2**, focusing specifically on the current adoption, controller platforms, and main deployment environments. From the results, it can be observed that 43.4% of the participants had fully adopted SDN, 40.6% had partially adopted the technology, while 16.0% were in the pilot stage of the SDN adoption. Regarding controllers' platform, Cisco ACI platform was the most common (33.1%) followed by VMware NSX (23.4%), Open Daylight (18.9%), and Juniper Contrail (12.6%). From Table 2, it is evident that the main deployment environment for SDN technology was the enterprise LANs (46.9%) followed by data centers (26.9%), WANs (16.0%), and hybrid clouds (10.2%).

### 3.3 Organizational Benefits of SDN Adoption




| | Improved Network Agility | Reduced Network Downtime | Better Traffic Engineering | Enhanced Security Policy | Faster Service Provisioning | Reduced Operational Cost | Simplified Network Management | Better Cloud Integration |
|---|---|---|---|---|---|---|---|---|
| Yes (%) | 89.1 | 82.3 | 86.9 | 84 | 88.6 | 76 | 87.4 | 83.4 |
| No (%) | 10.9 | 17.7 | 13.1 | 16 | 11.4 | 24 | 12.6 | 16.6 |

**Figure 1.** Organizational Benefits of Software-Defined Networking Adoption

Benefits of the software-defined networking implementation to an organization according to the participants as shown in **Figure 1**. The findings show that increased network agility (89.1%) ranked the highest among the benefits, then fast service deployment (88.6%), easy network management (87.4%), and efficient traffic engineering (86.9%). In addition to this, there was an increase in security policies (84.0%), improved cloud integration (83.4%), and minimized network downtime (82.3%). The lowest benefit that scored the least in percentage was reduced operational cost (76.0%), but even this benefit was observed to be significant to many participants. As evident from Figure 1, software-defined networking has many positive impacts on the efficiency and performance of an organization.

3.4 Primary Challenges of Software-Defined Networking Adoption

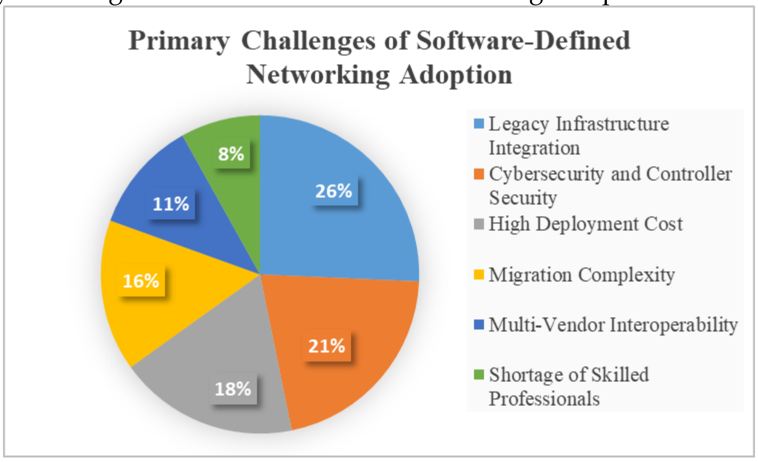



**Figure 2**. Primary Challenges of Software-Defined Networking Adoption

In Figure 2 below shows the main challenges experienced when adopting software-defined networking. The biggest challenge reported was legacy infrastructure integration (25.7%). This is due to the difficulties that exist when trying to integrate new SDN architectures into existing networks. Other challenges included cyber security and controller security (21.1%) and expensive deployment cost (18.3%). These two are associated with security and cost of implementation of software-defined networking respectively. Migration challenges (15.4%) posed another problem in the implementation process. Multi-vendor interoperability (11.4%) and lack of expertise (8.1%) are also some of the problems associated with software-defined networking adoption.

3.5 Pearson Correlation Matrix of the Study Variables

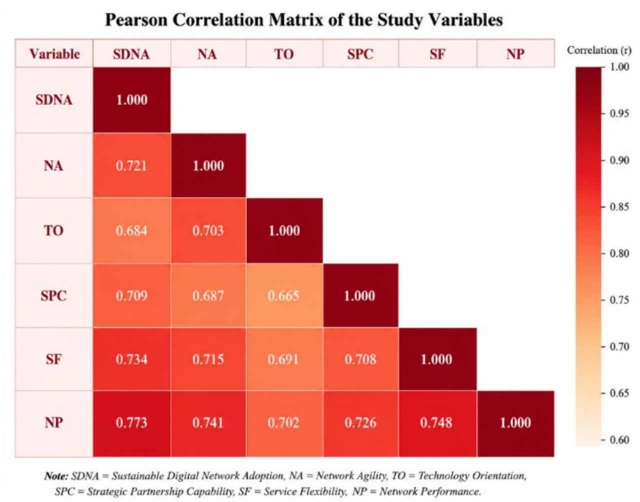



**Figure 3.** Pearson Correlation Matrix of the Study Variables

Pearson correlation coefficients for all the variables of this study show a significant and positive correlation among each other as seen in **Figure 3**. The highest correlation was found between SDN adoption and network performance (r=0.773), followed by scalability and flexibility (r=0.748), network automation (r=0.741), security and policy control (r=0.726), and traffic optimization (r=0.702). Moreover, the independent variables themselves had some positive correlation among each other as well, where correlation coefficients varied from 0.665 to 0.734, suggesting that there is no presence of any excessive multi-collinearity. Figure 3 implies that improvements in software-defined networking lead to better network performance and networking efficiency.

3.6 Multiple Regression Analysis

**Table 3**. Multiple Regression Analysis

| Predictor | β | SE | Standardized β | t | p |
|---|---|---|---|---|---|
| Constant | 0.492 | 0.318 | — | 1.55 | 0.123 |
| SDNA | 0.284 | 0.051 | 0.298 | 5.57 | <0.001 |
| NA | 0.237 | 0.048 | 0.256 | 4.94 | <0.001 |
| TO | 0.169 | 0.046 | 0.183 | 3.67 | <0.001 |
| SPC | 0.194 | 0.049 | 0.211 | 3.96 | <0.001 |
| SF | 0.221 | 0.052 | 0.229 | 4.25 | <0.001 |
| **Model Summary** | | | | | |
| Statistic | | | | Value | |
| R | | | | 0.857 | |
| $R^2$ | | | | 0.734 | |
| Adjusted $R^2$ | | | | 0.726 | |
| F | | | | 93.47 | |
| p-value | | | | <0.001 | |
| Durbin-Watson | | | | 2.04 | |

The results of the regression in **Table 3** show that the model we proposed is very good at explaining how well the network performs. We got an R of 0.857 an $R^2$ of 0.734 and an Adjusted $R^2$ of 0.726. This means that the multiple regression results can explain 73.4 percent of the variation in network performance. The study variables are the things that affect network performance. The overall model is statistically significant with an F of 93.47 and a p value of than 0.001. The Durbin-Watson value is 2.04 which means there is no autocorrelation. When we look at the things that affect network performance we see that software-defined network adoption has the positive effect on network performance with a beta of 0.298 and a p value of less than 0.001. Network automation is next with a beta of 0.256. Then we have scalability and flexibility with a beta of 0.229, security and policy control with a beta of 0.211 and traffic optimization, with a beta of 0.183. These results tell us that software-defined network adoption, network automation, scalability and flexibility security and policy control and traffic optimization all contribute to making network performance.

3.7 Hypothesis Testing Results for the Proposed Research Model

**Table 4.** Hypothesis Testing Results for the Proposed Research Model

| Hypothesis | Path | β | t | p | Decision |
|---|---|---|---|---|---|
| H1 | SDNA → NP | 0.298 | 5.57 | <0.001 | Supported |
| H2 | NA → NP | 0.256 | 4.94 | <0.001 | Supported |
| H3 | TO → NP | 0.183 | 3.67 | <0.001 | Supported |

| Hypothesis | Path | β | t | p | Decision |
|---|---|---|---|---|---|
| H4 | SPC → NP | 0.211 | 3.96 | <0.001 | Supported |
| H5 | SF → NP | 0.229 | 4.25 | <0.001 | Supported |

The results of the hypothesis testing are shown in **Table 4**. This table shows that all the ideas we thought might be true were actually supported by the numbers. When we looked at how different things affected the network we found that using software-defined networks had the positive effect on how well the network worked. This means that software-defined network adoption is very important for network performance. The numbers were pretty clear on this: β was 0.298 t was 5.57 and p was than 0.001. This supports the idea that software-defined networkers a good thing, which we called H1. We also found that automating the network was important which we called H2. Being able to scale and be flexible was important to which we called H5. Having security and control over policies was important which we called H4. Optimizing traffic was important which we called H3. All of these things had an effect on the network and the numbers were statistically significant meaning they were not just random. As you can see in Table 4 these results support the model we proposed for research. They also show that making software-defined networking better can really improve how well the network works in companies and places that provide services. This is a deal, for enterprise and service provider environments.

## 4. Discussion

The results of this study show that software-defined networking is becoming more and more important for enterprise and service provider networks. Organizations are moving away from network setups and towards ones that are programmable and managed from a central point [22]. What is really interesting is that 43.4% of the organizations that took part in the study have already fully implemented software-defined networking, which shows that it is being accepted as a way to deal with the complexity of modern communication networks. The fact that software-defined networking is being adopted widely shows that there is a need for network management that is flexible can be scaled up and is intelligent so it can support cloud computing, virtualization and the fast-changing digital services [23]. The people who responded to the study were experienced networking professionals, which makes the results more credible and provides a realistic view of how software-defined networking is being used in the real world [24].

The benefits that organizations think they get from software-defined networking show that it has value in networking environments. The biggest benefit that organizations agree on is that it improves network agility, with 89.1% of respondents saying this which means that organizations are really valuing the ability to quickly respond to changes, in business and technology. Respondents also said that software-defined networking improves the way services are provided, network management, traffic engineering, security policies, cloud integration and operational efficiency [25]. These results suggest that having a central network intelligence allows organizations to make administrative processes simpler while also improving network visibility and how resources are allocated. Software-defined networking is not just replacing networking it is providing a flexible platform that can support automation, new services and digital transformation [26]. Overall the responses show that organizations think the main result of implementing software-defined networking is that it improves operations and financial benefits become more clear as it is used more.

The study found that the benefits of software-defined networking were really good. It also found some problems that are still stopping companies from using it. One of the problems is getting old systems to work with new ones. It is hard to move from hardware to new programmable networks. There are also concerns about cybersecurity how much it costs to set it up how hard it is to move to the system and if different systems can work together [27]. Companies also need to have people who know what they are doing. All these problems show that companies need to be ready and have the technology to make software-defined networking work. To do it successfully companies need to plan have a standard way of setting it up take care of cybersecurity and keep training their workers [28]. Companies should also do it in stages so they do not disrupt their operations. They need to make sure their old systems work with the software-defined network systems. Statistical analysis supports the idea that software-defined networking's a good thing [29]. It shows that the more companies use software-defined networking, the better their networks work. This is shown by a number called $\beta = 0.298$ which means that using software-defined networking directly improves how well companies' networks work. The analysis explains why networks work better and it shows that the things that were studied are important [30]. The study also found that automating networks optimizing traffic keeping them secure and making them scalable are all important, for making software-defined networking work. These things help companies work better. The study shows that companies should not just focus on setting up technology but also on automating and securing their networks and making them work well.

## 5. Conclusion

This study shows that software-defined networking really makes a difference in how well networks work in companies and places that provide services. It does this by making things automatic so people do not have to do everything by hand. It gives people more control, over the network from one place. The study found out that using software-defined networks is the way to make networks work better. All the other things they looked at also helped companies do better. Companies can use software-defined networking to make sure they have networks that will support them as they change and grow.

## REFERENCES


[1] T. Bakhshi, "State of the art and recent research advances in software defined networking," Wireless Communications and Mobile Computing, vol. 2017, pp. 1–35, 2017, doi: 10.1155/2017/7191647.

[2] S. Singh and R. K. Jha, "A survey on Software Defined Networking: Architecture for Next Generation network," Journal of Network and Systems Management, vol. 25, no. 2, pp. 321–374, 2016, doi: 10.1007/s10922-016-9393-9.

[3] R. Horvath, D. Nedbal, and M. Stieninger, "A literature review on challenges and effects of software defined networking," Procedia Computer Science, vol. 64, pp. 552–561, 2015, doi: 10.1016/j.procs.2015.08.563.

[4] M. Yang, Y. Li, D. Jin, L. Zeng, X. Wu, and A. V. Vasilakos, "Software-defined and virtualized future mobile and wireless networks: A survey," Mobile Networks and Applications, vol. 20, no. 1, pp. 4–18, 2014, doi: 10.1007/s11036-014-0533-8.

[5] Y. Gong, W. Huang, W. Wang, and Y. Lei, "A survey on software defined networking and its applications," Frontiers of Computer Science, vol. 9, no. 6, pp. 827–845, 2015, doi: 10.1007/s11704-015-3448-z.

[6] Y. Li et al., "Enhancing the Internet of Things with knowledge-driven software-defined networking technology: Future perspectives," Sensors, vol. 20, no. 12, Art. no. 3459, 2020, doi: 10.3390/s20123459.

[7] K. Benzekki, A. E. Fergougui, and A. E. Elalaoui, "Software-defined networking (SDN): A survey," Security and Communication Networks, vol. 9, no. 18, pp. 5803–5833, 2016, doi: 10.1002/sec.1737.

[8] M. Chahal, S. Harit, K. K. Mishra, A. K. Sangaiah, and Z. Zheng, "A survey on software-defined networking in vehicular ad hoc networks: Challenges, applications and use cases," Sustainable Cities and Society, vol. 35, pp. 830–840, 2017, doi: 10.1016/j.scs.2017.07.007.

[9] Imran, Z. Ghaffar, A. Alshahrani, M. Fayaz, A. M. Alghamdi, and J. Gwak, "A topical review on machine learning, software defined networking, Internet of Things applications: Research limitations and challenges," Electronics, vol. 10, no. 8, Art. no. 880, 2021, doi: 10.3390/electronics10080880.

[10] A. K. Rangisetti and B. R. Tamma, "Software defined wireless networks: A survey of issues and solutions," Wireless Personal Communications, vol. 97, no. 4, pp. 6019–6053, 2017, doi: 10.1007/s11277-017-4825-8.

[11] F. X. Wibowo, M. A. Gregory, K. Ahmed, and K. M. Gomez, "Multi-domain software defined networking: Research status and challenges," Journal of Network and Computer Applications, vol. 87, pp. 32–45, 2017, doi: 10.1016/j.jnca.2017.03.004.

[12] M. U. Younus, S. U. Islam, I. Ali, S. Khan, and M. K. Khan, “A survey on software defined networking enabled smart buildings: Architecture, challenges and use cases,” Journal of Network and Computer Applications, vol. 137, pp. 62–77, 2019, doi: 10.1016/j.jnca.2019.04.002.
[13] K. M. Modieginyane, B. B. Letswamotse, R. Malekian, and A. M. Abu-Mahfouz, “Software defined wireless sensor networks application opportunities for efficient network management: A survey,” Computers & Electrical Engineering, vol. 66, pp. 274–287, 2017, doi: 10.1016/j.compeleceng.2017.02.026.
[14] Z. Yan, P. Zhang, and A. V. Vasilakos, “A security and trust framework for virtualized networks and software-defined networking,” Security and Communication Networks, vol. 9, no. 16, pp. 3059–3069, 2015, doi: 10.1002/sec.1243.
[15] W. Bekri, R. Jmal, and L. C. Fourati, “Internet of Things management based on software defined networking: A survey,” International Journal of Wireless Information Networks, vol. 27, no. 3, pp. 385–410, 2020, doi: 10.1007/s10776-020-00488-2.
[16] Y. Jararweh, M. Al-Ayyoub, A. Darabseh, E. Benkhelifa, M. Vouk, and A. Rindos, “Software defined cloud: Survey, system and evaluation,” Future Generation Computer Systems, vol. 58, pp. 56–74, 2015, doi: 10.1016/j.future.2015.10.015.
[17] B. Isyaku, M. S. M. Zahid, M. B. Kamat, K. A. Bakar, and F. A. Ghaleb, “Software defined networking flow table management of OpenFlow switches performance and security challenges: A survey,” Future Internet, vol. 12, no. 9, Art. no. 147, 2020, doi: 10.3390/fi12090147.
[18] R. Buyya and J. Son, “Software-defined multi-cloud computing: A vision, architectural elements, and future directions,” in Lecture Notes in Computer Science, pp. 3–18, 2018, doi: 10.1007/978-3-319-95162-1_1.
[19] Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, and M. Imran, “Security in software-defined networking: Threats and countermeasures,” Mobile Networks and Applications, vol. 21, no. 5, pp. 764–776, 2016, doi: 10.1007/s11036-016-0676-x.
[20] I. M. Alsmadi, I. AlAzzam, and M. Akour, “A systematic literature review on software-defined networking,” in Studies in Computational Intelligence, pp. 333–369, 2016, doi: 10.1007/978-3-319-44257-0_14.
[21] Z. AlSaeed, I. Ahmad, and I. Hussain, “Multicasting in software defined networks: A comprehensive survey,” Journal of Network and Computer Applications, vol. 104, pp. 61–77, 2017, doi: 10.1016/j.jnca.2017.12.011.
[22] A. Razzaq, “A systematic review on software architectures for IoT systems and future direction to the adoption of microservices architecture,” SN Computer Science, vol. 1, no. 6, 2020, doi: 10.1007/s42979-020-00359-w.
[23] A. M. Abdelrahman, J. J. P. C. Rodrigues, M. M. E. Mahmoud, K. Saleem, A. K. Das, V. Korotaev, and S. A. Kozlov, “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, 2020, doi: 10.1002/dac.4706.
[24] R. F. Babiceanu and R. Seker, “Cyber resilience protection for industrial internet of things: A software-defined networking approach,” Computers in Industry, vol. 104, pp. 47–58, 2018, doi: 10.1016/j.compind.2018.10.004.
[25] W. Li, W. Meng, and L. F. Kwok, “A survey on OpenFlow-based software defined networks: Security challenges and countermeasures,” Journal of Network and Computer Applications, vol. 68, pp. 126–139, 2016, doi: 10.1016/j.jnca.2016.04.011.
[26] N. Al-Mi’ani, M. Anbar, Y. Sanjalawe, and S. Karuppayah, “Securing software defined networking using intrusion detection system—A review,” in Communications in Computer and Information Science, pp. 417–446, 2021, doi: 10.1007/978-981-16-8059-5_26.
[27] L. M. Contreras, L. Cominardi, H. Qian, and C. J. Bernardos, “Software-defined mobility management: Architecture proposal and future directions,” Mobile Networks and Applications, vol. 21, no. 2, pp. 226–236, 2016, doi: 10.1007/s11036-015-0663-7.
[28] J. Šuh, Ž. Bojović, M. Despotović-Zrakić, Z. Bogdanović, and A. Labus, “Designing a course and infrastructure for teaching software-defined networking,” Computer Applications in Engineering Education, vol. 25, no. 4, pp. 554–567, 2017, doi: 10.1002/cae.21820.
[29] T. Semong, T. Maupong, S. Anokye, K. Kehulakae, S. Dimakatso, G. Boipelo, and S. Sarefo, “Intelligent load balancing techniques in software defined networks: A survey,” Electronics, vol. 9, no. 7, Art. no. 1091, 2020, doi: 10.3390/electronics9071091.
[30] N. Dayal, P. Maity, S. Srivastava, and R. Khondoker, “Research trends in security and DDoS in SDN,” Security and Communication Networks, vol. 9, no. 18, pp. 6386–6411, 2016, doi: 10.1002/sec.1759.