Security of Infocommunication Systems and Internet of Things

2025 Vol 3, No 1

https://doi.org/10.31861/sisiot2025.1.01011

Received 05 June 2025; revised 27 June 2025; accepted 29 June 2025; published 30 June 2025

AI-enabled Cloud SDN Controllers: Architecture, Scalability, and Security – A Comparative Study

Anatolii Banar[1,*] and Heorhii Vorobets[2]

[1]Radio Engineering and Information Security Department, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine
[2]Computer Systems and Networks Department, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine

*Corresponding author (E-mail: banar.anatolii@chnu.edu.ua)

ABSTRACT This article investigates the applicability and advantages of deploying a software-defined networking (SDN) controller within a cloud infrastructure. The study begins by analyzing the architectural differences between on-premises SDN controllers and cloud-based implementations, including monolithic, microservice, and hybrid edge-cloud approaches. The motivation is driven by the need to address modern network challenges such as dynamic scalability, efficient control over geographically distributed systems, and the integration of advanced automation tools. Cloud-based SDN controllers offer more convenient maintenance and seamless integration with external services, including telemetry, monitoring, and DevOps pipelines, than their locally deployed counterparts. However, they also introduce latency concerns and potential risks related to data confidentiality, which must be mitigated through encryption and secure communication protocols. The article emphasizes the integration of artificial Intelligence (AI) into the control plane. AI-powered modules enable the prediction of traffic patterns, detection of network anomalies, dynamic adjustment of routing policies, and overall improvement in quality of service. Examples from recent research, including implementations such as TeraFlowSDN, demonstrate the viability of embedding machine learning components within cloud-hosted controllers to enhance their decision-making capabilities. Comparative evaluation demonstrates that cloud deployment is preferable in contexts such as IoT-oriented systems or rapidly evolving network infrastructures. Properly designed, cloud-based SDN controllers can deliver performance levels comparable to traditional systems while offering greater flexibility for future development and integration with intelligent network services.

KEYWORDS software-defined networking, cloud infrastructure, artificial intelligence, quality of service, resource constraints.

I. INTRODUCTION

Software-defined networking (SDN) is an approach to designing, managing, and operating computer networks [1] that separates data forwarding plane from the control plane, enabling centralized traffic administration through a programmable controller. In this model, network control logic resides in a centralized, software-based controller, while network devices (e.g., routers and switches) execute provided by this controller instructions. Typically, the SDN controller is deployed locally, either within enterprise-owned servers or data centers, directly interacting with network equipment.

With the rapid evolution of cloud technologies, deploying SDN controllers in a cloud environment has emerged as an alternative worth exploring. A cloud-based SDN controller [2] involves the deployment of network control logic within a virtualized cloud infrastructure (e.g., Cisco Meraki, Cradlepoint NetCloud, Azure, or private clouds), providing remote management of network devices through secure communication channels. The ongoing proliferation of IoT devices, intelligent nodes, and the widespread adoption of 5G technologies pose new challenges for network management. Although centralized control inherent to SDN already offers substantial flexibility and global oversight, the ability of cloud-based implementations [2] to enhance or at least preserve these advantages relative to traditional SDN controllers remains a critical issue, necessitating further investigation within practical cloud environments.

Moreover, recent trends underline the necessity of integrating artificial intelligence (AI) into network architectures, making AI an essential consideration when selecting the architecture of an SDN-based network.

II. ANALYSIS OF RECENT RESEARCH AND PUBLICATIONS

Researchers have shown considerable interest in utilizing SDN technologies for IoT and 5G networks. For instance, in study [3], a hierarchical controller system known as Hierarchical Edge-Cloud SDN (HECSDN) has been proposed. This system integrates a central controller deployed in the cloud with local controllers situated at network edges to enhance scalability. Such architecture mitigates the risk of overloading a single controller by distributing computational tasks between the cloud and edge environments, thus ensuring efficient performance in extensive network deployments.

Further research, presented in [4, 5], examines SDN implementations within IoT and smart city contexts, highlighting aspects of security and quality of service (QoS). Specifically, an overview of SDN architectures tailored for smart city applications [4] emphasizes the capability of centralized SDN controllers to implement security mechanisms and manage QoS effectively. The study points out that prominent industry players already provide cloud-based SDN solutions, such as the Ericsson Cloud SDN Controller, underscoring the real-world applicability and importance of these solutions.

Additionally, study [5] introduces a two-tier SDN architecture for IoT data management, demonstrating that combining local and cloud controllers accelerates data processing and reduces latency compared to solely cloud-based configurations. This research concludes that IoT environments with strict latency requirements benefit significantly from integrating the strengths of cloud infrastructures (robust processing capabilities, comprehensive network visibility) with the rapid response times offered by edge controllers.

The use of a single cloud-based controller poses challenges when managing numerous IoT nodes, primarily due to high communication overhead. Study [6] addresses this issue by proposing an architecture that distributes network intelligence among multiple controllers. This decentralized approach enhances fault tolerance and operational performance by enabling decision-making to be closer to data origins while preserving centralized oversight. Consequently, this distributed cloud model effectively resolves limitations inherent in a centralized cloud by incorporating edge computing nodes [7]. These edge nodes feature low latency and offer preliminary local data processing capabilities.

At the same time, research efforts are focused on integrating artificial intelligence into cloud-based SDN controllers. The European Telecommunications Standards Institute (ETSI) introduced TeraFlowSDN, an open project centered on a microservices-based SDN controller with built-in machine learning modules. In study [8], the implementation of an ML-driven cybersecurity component within the TeraFlowSDN controller is described, showcasing its capability to detect network intrusions and malicious activities effectively. The significance of cloud-native practices such as containerization and Kubernetes-based orchestration for building adaptable SDN controllers has been thoroughly examined in recent studies [9, 10]. This approach facilitates independent scaling and updating of individual microservices, distributing workloads among service replicas, eliminating single points of failure, and simplifying system maintenance.

Therefore, cloud-based SDN controllers have garnered significant research attention in recent years. Earlier research predominantly concentrated on validating the feasibility and basic functionality of cloud-deployed controllers. The research emphasis has transitioned towards optimizing architectural frameworks (particularly microservices architectures) and enhancing integration capabilities with AI technologies.

III. ARCHITECTURE OF SDN CONTROLLERS AND THEIR CLOUD IMPLEMENTATIONS

A **SDN Controller** represents a monolithic hardware-software system, or a closely integrated modular software solution deployed on a single server or a server cluster within an SDN network (Fig. 1). Prominent examples include open-source implementations such as OpenDaylight, ONOS, and Ryu. These controllers feature Southbound APIs (such as OpenFlow) for communication with network devices, and Northbound APIs, which allow policy management of programmable switches [11].

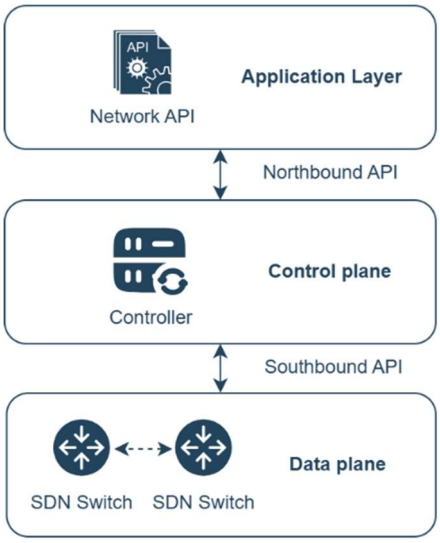

FIG. 1. SDN network structure.

Controller scaling can be implemented vertically, by increasing the hardware resources of a single server, or horizontally, by creating clusters consisting of multiple controller instances that synchronize network states between themselves. Nevertheless, horizontal clustering introduces additional complexity into the system [12], necessitates mechanisms for state synchronization, and typically supports only a limited number of nodes effectively. Consequently, the conventional SDN controller architecture encounters scalability constraints under substantial load conditions, where limited computational resources can lead to delays in handling requests and updating flow tables.

A **Cloud-based SDN Controller** is an implementation of the SDN control plane deployed within a cloud infrastructure (Fig. 2), which can be private, public, or hybrid.

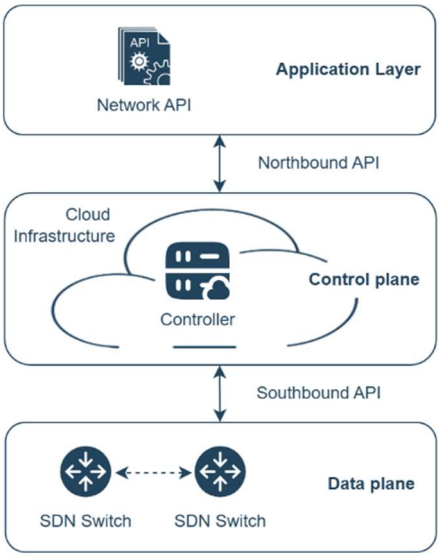

FIG. 2. SDN network structure with a cloud-based controller.

Several architectural approaches exist for deploying such a controller:

A. Cloud-based Monolithic Architecture is deploying the same SDN controller software on a cloud server as used in an on-premises scenario. This enables centralized

management of geographically distributed networks (e.g., enterprise networks) without the need to operate proprietary data centers. Commercial examples of this approach include Cisco Meraki and TP-Link Omada, both offering cloud-managed network platforms that effectively function as SDN controllers for client network infrastructure.

B. Microservice (Cloud-Native) Architecture solutions such as ETSI`s TeraFlowSDN redesign the SDN controller specifically for cloud deployment by decomposing it into multiple microservices. Each microservice is dedicated to a distinct functional aspect, such as topology management, security management, routing control, or traffic analytics. These microservices are containerized and orchestrated using Kubernetes [9], enabling automatic scaling, seamless updates without network disruptions (allowing multiple controller versions to run concurrently), and enhanced fault tolerance.

C. Hierarchical (Edge-Cloud) Architecture combines the strengths of both local and cloud-based SDN controllers. At the upper level of this hierarchy is a global cloud-based controller, which owns a comprehensive view of the entire network and manages high-level operations such as security policies and cross-domain routing decisions [3]. At the lower level are local controllers, typically implemented as compact devices or virtual machines located at network edges. Each local controller manages a specific network segment, such as a bank`s local network or an IoT subnetwork within a city and handles real-time operational tasks. Local controllers communicate with the global controller by transmitting aggregated data and, in return, receive global instructions that they implement locally.

A comparative overview of architectural distinctions between locally deployed and cloud-hosted SDN controllers is presented in Table 1.

TABLE 1. Cloud-Based SDN and On-Premises and Controller Architectures Comparison.

Criteria	On-Premises	Cloud-Based
Architecture	Monolithic or clustered within the local network	Remote (microservices, containers, orchestration)
Deployment	Local (within the organization)	Cloud infrastructure (private/public)
Latency	Minimal (due to proximity to network nodes)	Higher, dependent on internet connection
Scalability	Limited, manual (vertical scaling or small-scale clustering)	Flexible, automatic horizontal scaling through service instance replication
Fault Tolerance	Requires on-site backup controller	Built-in via cloud-native mechanisms
Maintenance	Downtimes during updates	Gradual, independent updates

An on-premises implementation is well-suited for small to medium-sized networks with low latency requirements but lacks scalability for large-scale or globally distributed systems. In contrast, cloud-based architecture introduces an additional layer of abstraction, which may lead to increased latency, but significantly simplifies the management of distributed infrastructures and effectively addresses scalability challenges. Modern cloud-native approaches enable the development of flexible SDN controllers that support seamless upgrades and integration of emerging services such as artificial intelligence and advanced analytics.

IV. COMPARISON OF IMPLEMENTATIONS BY CRITERIA

Let us examine in more detail the key criteria used to evaluate the differences between cloud-based and on-premises SDN controllers:

Scalability. Cloud-based controllers offer superior scalability due to dynamic resource provisioning [13]. As the number of connected devices or the volume of traffic increases, resources such as CPU cores, memory, or service instances can be rapidly scaled up on demand. In contrast, on-premises controllers are constrained by the physical limitations of dedicated hardware. Scaling requires the acquisition and installation of new equipment, as well as configuring clusters, processes that are often time-consuming and inflexible.

Cost. One of the most apparent distinctions lies in the difference between Capital Expenditures (CapEx) and Operating Expenses (OpEx). On-premises deployment requires upfront investment in hardware, physical space, power supply, and a dedicated person for maintenance, all of which contribute to substantial CapEx. This approach may be justified for networks operating under consistently high load conditions. In contrast, the cloud-based model shifts spending toward OpEx, where users pay for rented resources and actual usage. For small and medium-sized networks, this model can be more cost-effective, as expenses are tied to actual consumption, and idle resources incur minimal cost. Additionally, automation in cloud environments helps reduce ongoing maintenance overhead.

However, in the long term, extensive reliance on cloud infrastructure can become more expensive than a one-time investment in on-premises hardware. Moreover, mission-critical networks may require private cloud deployments to meet specific security or performance requirements, which further increases operational costs.

Latency is one of the most sensitive parameters. When the SDN controller is deployed locally, the latency between the network switch and the controller is minimal, typically just a few milliseconds or even less within a local network. However, if the controller resides in a remote cloud data center, potentially located hundreds or even thousands of kilometers away, additional communication delays become inevitable. This increased latency can impact the time required to establish new flows (e.g., TCP / UDP sessions) or respond to network events, such as the enforcement of newly defined security policies.

As a mitigation strategy, hybrid architecture may be employed [14], wherein time-critical decisions are made

locally at the edge, while non-critical or delay-tolerant tasks are offloaded to the cloud.

Flexibility and Integration with other technologies. Cloud-based SDN controllers offer a distinct advantage in terms of flexibility and interoperability. They can be seamlessly integrated with orchestration platforms such as OpenStack and Kubernetes [15], as well as with monitoring, logging, and DevOps tools. Furthermore, cloud controllers commonly expose standardized APIs (e.g., REST, gRPC) for third-party applications, facilitating the development of customized network services. While traditional on-premises controllers may also provide APIs, they are often less standardized and tailored for local deployment scenarios. In contrast, a cloud environment enables the creation of unified portals or platforms for software-defined network management across multiple organizational departments or even distinct clients.

Security. In an on-premises SDN deployment, administrators maintain full control over the physical infrastructure, which simplifies tasks such as auditing, network segmentation, and securing internal communication channels. However, responsibility for maintaining system security, including applying patches, monitoring threats, and performing updates, rests entirely with the local IT team. Cloud providers, on the other hand, typically deliver high levels of both physical and cybersecurity protection, along with regular updates that help mitigate vulnerabilities. Nonetheless, cloud-based architecture introduces new security concerns [16], since communication between the controller and network devices occurs over external channels, robust encryption and authentication mechanisms, such as TLS for OpenFlow, are essential.

V. AI INTEGRATION INTO CLOUD-BASED SDN CONTROLLERS

One of the important advantages of deploying the SDN controller within a cloud-native environment is the enhanced potential for seamless integration with AI and machine learning (ML) tools. AI can significantly augment SDN controllers` functionality, enabling more adaptive and intelligent network behavior.

Below are several areas in which AI is currently being applied or actively researched in the context of cloud-based SDN:

A. Traffic Forecasting and Optimization. Machine learning techniques enable predictive network load analysis, such as anticipating peak traffic periods throughout the day, and allowing proactive network reconfiguration. Cloud-based SDN controllers offer sufficient computational capacity to support deep learning models execution for such forecasting tasks. In transport network environments, existing solutions [10, 17] have demonstrated how cloud-native SDN controllers can integrate traffic prediction modules to redistribute bandwidth across optical links dynamically. This approach improves resource utilization and enhances QoS for end users.

B. Cyberattack Detection and Response. A cloud-based controller benefits from a global view of network traffic, making it well-suited for implementing intrusion detection and prevention systems (IDS / IPS). Integration with AI enables the detection of anomalous traffic patterns and supports real-time response mechanisms.

Embedded AI modules within the controller can dynamically update security policies in reaction to evolving attack behaviors, thereby minimizing the impact on network performance [18]. By leveraging deep learning models, the controller can perform real-time traffic analysis with significantly improved accuracy in detecting Distributed Denial of Service (DDoS) attacks within SDN networks [19].

C. QoS and Service Management. Artificial intelligence enhances the controller's ability to classify network traffic and make informed decisions regarding the prioritization or denial of service for specific flows. It also improves overall QoS through automated traffic control, dynamic resource allocation, and real-time adaptation to changing network conditions [20, 21]. For instance, using neural networks, the controller can distinguish between video streams and web traffic, reserving bandwidth according to traffic type.

D. Scalability and Network Sustainability. SDN provides a flexible, scalable platform for complex network configurations, while AI complements it by defining self-adaptive policies in real time. For example, a hierarchical reinforcement learning control scheme can distribute decision-making across multiple layers of controllers [22], enhancing the network's scalability without sacrificing performance. However, there remains a need to develop novel AI-based approaches [20] to address challenges in flow table management and controller clustering, as well as to establish precise criteria for evaluating the effectiveness of these algorithms.

Cloud-based SDN controllers offer the flexibility to integrate AI modules on demand by leveraging the elastic computing resources of cloud infrastructure, without the need to upgrade or expand local hardware. This is a notable advantage over on-premises deployments. Furthermore, thanks to microservice-based architecture, AI components can operate in parallel with the core control functions without interference. As a result, AI cloud-based SDN controllers` integration is already proven valuable in practice, ranging from enhanced network security to intelligent, self-optimizing responses to dynamic traffic conditions.

VI. CONCLUSION

Deploying an SDN controller within a cloud infrastructure represents a promising direction for addressing many of the limitations associated with traditional on-premises implementations. A cloud-based SDN controller offers improved scalability, greater flexibility in integrating new features, simplified centralized management of distributed networks, and native support for AI integration. However, the key concerns remain related to security and latency. Shifting control to the cloud requires network operators to place trust in external service providers. Consequently, all communication channels between the controller and network devices must be strongly encrypted, with robust authentication and access control mechanisms.

Literature review confirms that, when properly designed, cloud-based SDN architectures can deliver performance comparable to traditional solutions. Metrics such as latency and bandwidth can remain within acceptable bounds, particularly when hybrid architectures employing edge controllers are used to handle delay-sensitive segments.

Furthermore, AI cloud-based SDN environments integration contributes to improved service quality through automated traffic orchestration and adaptive resource management in dynamic network conditions.

AUTHOR CONTRIBUTIONS

A.B. – investigation, visualization, writing (original draft preparation); H.V. – supervision, writing (review and editing).

COMPETING INTERESTS

The authors declare no competing interests.

REFERENCES

[1] M. Priyadarsini and P. Bera, "Software defined networking architecture, traffic management, security, and placement: A survey," *Computer Networks*, vol. 192, p. 108047, 2021, doi: 10.1016/j.comnet.2021.108047.

[2] C. Manso, R. Vilalta, R. Casellas, R. Martinez, and R. Muñoz, "Cloud-native SDN Controller Based on Micro-Services for Transport Networks," in *Proc. IEEE Int. Conf. Network Softwarization (NetSoft)*, 2020, pp. 365–367, doi: 10.1109/NetSoft48620.2020.9165377.

[3] F. P.-C. Lin and Z. Tsai, "Hierarchical Edge-Cloud SDN Controller System With Optimal Adaptive Resource Allocation for Load-Balancing," *IEEE Systems Journal*, vol. 14, no. 1, pp. 265–276, Mar. 2020, doi: 10.1109/JSYST.2019.2894689.

[4] M. Rahouti, K. Xiong, and Y. Xin, "Secure Software-Defined Networking Communication Systems for Smart Cities: Current Status, Challenges, and Trends," *IEEE Access*, pp. 12083–12113, 2020, doi: 10.1109/ACCESS.2020.3047996.

[5] Z. Eghbali and L. Zolfy, "A hierarchical approach for accelerating IoT data management process based on SDN principles," *Journal of Network and Computer Applications*, vol. 181, 2021, doi: 10.1016/j.jnca.2021.103027.

[6] R. Firouzi and R. Rahmani, "A Distributed SDN Controller for Distributed IoT," *IEEE Access*, vol. 10, pp. 42873–42882, 2022, doi: 10.1109/ACCESS.2022.3168299.

[7] I. E. Kamarudin, M. Ameedeen, M. Faizal, and A. Zabidi, "Integrating Edge Computing and Software Defined Networking in Internet of Things: A Systematic Review," *Iraqi Journal for Computer Science and Mathematics*, vol. 4, pp. 121–150, 2023, doi: 10.52866/ijcsm.2023.04.04.011.

[8] A. Mozo, A. Karamchandani, L. la Cal, S. Gómez-Canaval, A. Pastor, and L. Gifre, "A Machine-Learning-Based Cyberattack Detector for a Cloud-Based SDN Controller," *Applied Sciences*, vol. 13, 2023, doi: 10.3390/app13084914.

[9] R. Pérez, M. Rivera, Y. Salgueiro, C. R. Baier, and P. Wheeler, "Moving Microgrid Hierarchical Control to an SDN-Based Kubernetes Cluster: A Framework for Reliable and Flexible Energy Distribution," *Sensors*, vol. 23, p. 3395, 2023, doi: 10.3390/s23073395.

[10] D. Adanza, L. Gifre, P. Alemany, J.-P. Fernández-Palacios, O. González-de-Dios, R. Muñoz, and R. Vilalta, "Enabling traffic forecasting with cloud-native SDN controller in transport networks," *Computer Networks*, vol. 250, p. 110565, 2024, doi: 10.1016/j.comnet.2024.110565.

[11] M. Diouf, S. Ouya, J. Klein, and T. Bissyandé, "Software Security in Software-Defined Networking: A Systematic Literature Review," *arXiv preprint* arXiv:2502.13828, 2025, doi: 10.48550/arXiv.2502.13828.

[12] R. Yujie, W. Muqing, and C. Yiming, "An Effective Controller Placement Algorithm Based on Clustering in SDN," in *Proc. IEEE 6th Int. Conf. Computer and Communications (ICCC)*, Chengdu, China, 2020, pp. 2294–2299, doi: 10.1109/ICCC51575.2020.9345045.

[13] P. Krishnan, K. Jain, A. Aldweesh, et al., "OpenStackDP: a scalable network security framework for SDN-based OpenStack cloud infrastructure," *Journal of Cloud Computing*, vol. 12, art. no. 26, 2023, doi: 10.1186/s13677-023-00406-w.

[14] S. Pal, N. Z. Jhanjhi, A. S. Abdulbaqi, D. Akila, A. A. Almazroi, and F. S. Alsubaei, "A Hybrid Edge-Cloud System for Networking Service Components Optimization Using the Internet of Things," *Electronics*, vol. 12, 2023, doi: 10.3390/electronics12030649.

[15] M. He, A. M. Alba, E. Mansour, and W. Kellerer, "Evaluating the Control and Management Traffic in OpenStack Cloud with SDN," in *Proc. IEEE 20th Int. Conf. High Performance Switching and Routing (HPSR)*, Xi'an, China, 2019, doi: 10.1109/HPSR.2019.8807989.

[16] I. Ivkic, D. Thiede, N. Race, and M. Broadbent, "Security Evaluation in Software-Defined Networks," *arXiv preprint* arXiv:2408.11486, 2024, doi: 10.48550/arXiv.2408.11486.

[17] O. Belkadi, A. Vulpe, Y. Laaziz, and S. Halunga, "ML-Based Traffic Classification in an SDN-Enabled Cloud Environment," *Electronics*, vol. 12, art. no. 269, 2023, doi: 10.3390/electronics12020269.

[18] I. Abdulqadder, S. Zhou, D. Zou, I. Aziz, and S. Akber, "Multi-layered Intrusion Detection and Prevention in the SDN/NFV Enabled Cloud of 5G Networks using AI-based Defense Mechanisms," *Computer Networks*, vol. 179, p. 107364, 2020, doi: 10.1016/j.comnet.2020.107364.

[19] Y. Al-Dunainawi, B. R. Al-Kaseem, and H. S. Al-Raweshidy, "Optimized Artificial Intelligence Model for DDoS Detection in SDN Environment," *IEEE Access*, vol. 11, pp. 106733–106748, 2023, doi: 10.1109/ACCESS.2023.3319214.

[20] M. R. Belgaum, Z. Alansari, S. Musa, M. Alam, and M. Mazliham, "Role of artificial intelligence in cloud computing, IoT and SDN: Reliability and scalability issues," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 5, pp. 4458–4470, 2021, doi: 10.11591/ijece.v11i5.pp4458-4470.

[21] M. Rostami and S. Goli-Bidgoli, "An overview of QoS-aware load balancing techniques in SDN-based IoT networks," *Journal of Cloud Computing*, vol. 13, art. no. 89, 2024, doi: 10.1186/s13677-024-00651-7.

[22] B. J. Ospina Cifuentes, Á. Suárez, V. García Pineda, R. Alvarado Jaimes, A. O. Montoya Benitez, and J. D. Grajales Bustamante, "Analysis of the use of artificial intelligence in software-defined intelligent networks: A survey," *Technologies*, vol. 12, art. no. 99, 2024, doi: 10.3390/technologies12070099.

Anatolii Banar

In 2015, graduated from Chernivtsi National University with a master`s degree in "Computer Systems and Networks". In 2022, entered postgraduate studies in the specialty "Telecommunications and radio engineering". Research interests include software-defined networks, programming, artificial intelligence.

ORCID ID: 0009-0006-7817-2058

Heorhii Vorobets

PhD, Associate Professor, Head of the Department of Computer Systems and Networks, Yuriy Fedkovych Chernivtsi National University. 2, Kotsyubynskogo Str., Chernivtsi, Ukraine, 58012.
E-mail: g.vorobets@chnu.edu.ua, phone: +38-0372-50-91-73

ORCID ID: 0000-0001-8125-2047

Хмарні SDN-контролери з підтримкою ШІ: архітектура, масштабованість та безпека (порівняльне дослідження)

Анатолій Банар[1,*], Георгій Воробець[2]

[1]Кафедра радіотехніки та інформаційної безпеки, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна
[2]Кафедра комп'ютерних систем та мереж, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна

*Автор-кореспондент (Електронна адреса: banar.anatolii@chnu.edu.ua)

АНОТАЦІЯ У статті досліджено потенціал хмарної реалізації SDN-контролера як альтернативи локальній моделі розгортання, в умовах динамічних викликів, що постають перед сучасними комп'ютерними мережами. Порівняльний аналіз проведено за ключовими критеріями - масштабованістю, затримками, гнучкістю, вартістю та безпекою. Наведено сучасні архітектурні підходи до побудови хмарних SDN-контролерів, такі як моноліт у хмарі, мікросервісні cloud-native рішення на базі Kubernetes, а також ієрархічні edge-cloud моделі. Показано, що хмарні контролери, завдяки віртуалізованому середовищу, мають кращі можливості до автоматичного масштабування, оновлення без зупинки системи, а також централізованого управління розподіленими мережами. Особливу увагу приділено інтеграції алгоритмів штучного інтелекту для підвищення рівня автоматизації управління мережею, прогнозування навантаження, адаптивного QoS та виявлення аномалій у трафіку. Розглянуто сценарії використання ШІ для прогнозування трафіку, виявлення DDoS-атак, автоматичного налаштування політик маршрутизації та покращення якості обслуговування. Виявлено, що хмарна інфраструктура створює сприятливі умови для запуску моделей глибокого навчання, які у випадку локального контролера важко реалізувати через обмеження ресурсів. При зваженому проектуванні хмарний SDN-контролер не лише не поступається локальному, а й має значний потенціал до масштабування, адаптації та інтеграції з інтелектуальними сервісами. Проте для критичних додатків із вимогами до мінімальних затримок рекомендовано використовувати гібридний підхід з edge-компонентами. Отримані результати можуть бути корисними при побудові сучасних розподілених мереж, зокрема в IoT-інфраструктурах, Smart City, або 5G-середовищах, де гнучкість, безперервне оновлення та інтелектуалізація управління є важливими завданнями.

КЛЮЧОВІ СЛОВА програмно-керовані мережі, хмарна інфраструктура, штучний інтелект, якість надання послуг, обмежені ресурси.