ISSN: 2182-2069 / E-ISSN: 2182-2077

Impact of Network Virtualization on Application Performance Metrics

Dr. Rami Ryad Hossein[1*], D.M. Malathi[2], Dr.M. Durgarani[3], Sudharsana Vijayan[4], T. Sriaruna Kameshwaran[5], and Dr. Priya Vij[6]

[1*]Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf of Al Diwaniyah, Al Diwaniyah, Iraq. iu.tech.eng.iu.comp.ramy_riad@iunajaf.edu.iq, https://orcid.org/0009-0009-5123-6949

[2]Assistant Professor, Department of Computer Science, Nallamuthu Gounder Mahalingam College, Pollachi, India. malathi.mca09@gmail.com, https://orcid.org/0000-0001-6744-072X

[3]School of Business and Management, Christ University, Karnataka, India. durgarani.m@christuniversity.in, https://orcid.org/0009-0004-1134-9336

[4]Assisstant Professor, Department of Electronics and communication Engineering, Vimal Jyothi Engineering College, Chemperi, Kannur, Kearla, India. sudharsanavijayan@vjec.ac.in, https://orcid.org/0009-0009-4817-3414

[5]Assistant Professor, Department of Master of Computer Applications, New Prince Shri Bhavani College of Engineering and Technology, Chennai, Tamil Nadu, India. sriaruna.mca@gmail.com, https://orcid.org/0009-0003-5325-4506

[6]Assistant Professor, Department of Computer Science, Kalinga University, Naya Raipur, Chhattisgarh, India. ku.priyavij@kalingauniversity.ac.in, https://orcid.org/0009-0005-4629-3413

Received: May 17, 2025; Revised: July 05, 2025; Accepted: August 08, 2025; Published: August 30, 2025

Abstract

The advent of network virtualization has redefined modern networking philosophies by allowing the partitioning of physical networks into virtual networks that are easily scalable, elastic, and efficient. The shift has been markedly critical to the function of applications in virtualized settings. This research examines the impact of network virtualization on key application performance indicators, including latency, throughput, packet loss, and resource utilization. The paper empirically assesses factors related to user experience and system performance by analyzing various virtualization technologies, including Software-Defined Networks (SDN), Network Functions Virtualization (NFV), and virtual overlay networks. The approach used entails deploying controlled benchmark applications on both virtualized and non-virtualized networks and measuring deviations from benchmark performance. Results indicate a strong correlation between the moderation of network performance overhead with virtualization and the presence of adaptive performance improvement schemes tailored to specific conditions. The efficiency of the hypervisor, placement of network functions, and orchestration policies significantly influence the responsiveness of the applications

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 3 (August), pp. 495-505. DOI: *10.58346/JISIS.2025.I3.034*

*Corresponding author: Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University in Najaf of Al Diwaniyah, Al Diwaniyah, Iraq.

Additionally, the paper addresses the increasing scalability limitations of performance in cloud-native and edge-computing environments. There is a finding that indicates increased need for research 'effective intelligent resource management and adaptive network reconfiguration strategies in order to minimize latency and redundant bandwidth allocation bottlenecks'.

Keywords: Network Virtualization, Application Performance, Latency, Throughput, SDN, NFV, Resource Utilization.

1 Introduction

This paper has examined how network virtualization affects the performance of legacy networks and SDN- and NFV-based networks in terms of application. The five KPI samples, applied based on the methodology strategy of conducting empirical testing and follow-up statistical analysis, comprised the following: latency, throughput, jitter, packet loss, and CPU utilization. Concerning the final product, latency, jitter, and resource sizing are indeed higher with virtualization, but the enhanced throughput, elasticity, and flexibility offset this. The specified scenario argues that, at the very least, when adequately adjusted, virtualized networks can be just as competent and potentially more efficient than traditional networks. The book focuses on how business corporations and service providers can apply virtualization technologies in modern computer environments. There is no way to hide the transition from fixed hardware-based infrastructures to software-based virtualized infrastructures due to the current spikes in data traffic and the dynamism of the services. However, the convenience of use and the design of the user interface do not mitigate the burden of managing numerous virtual layers which impacts application performance metrics, including, but not limited to, latency, throughput, and jitter (Kreutz et al., 2014; Lee et al., 2012).In a virtual network, the interaction between virtual components and hardware can lead to performance declines due to network delays, resource contention, and overhead, which can degrade latency-sensitive applications (Dizdarević et al., 2019).

The virtualization of infrastructure is becoming increasingly essential to the functioning of organizations; thus, understanding the analytical performance intricacies of such systems becomes critical (Praveenraj et al., 2024). The performance of applications, especially in data-intensive fields such as healthcare, finance, and IoT domains, is highly dependent on the operability and efficiency of the network (El Chall et al., 2018). In infrastructural networks, assessing system performance, particularly in virtualized networks, has become crucial for QoS, end-user satisfaction, and system dependability (Liu et al., 2021). The research problem is to fill the gap in the research on the advantages and feasibility of virtualized network by evaluating their performance in application (Foukas et al., 2017). Understanding the impact of virtualization on major performance metrics and deliberation constraint provisioning is useful for optimizing system performance. Therefore, it guides the tactical system design in the coordination of architecture of network and IT services (Ritthish et al., 2023; Ali & Bilal, 2025). There are highly scalable, flexible, and cost-effective virtual networks like Software-Defined Networking (SDN) and Network Functions Virtualization (NFV). However, the advantages are accompanied by critical security problems that must be addressed to ensure the virtualized networks operate securely and reliably. The controller is the most critical component in SDN because it serves as the control node of the network. Its compromise could lead to malicious control, unauthorized usage, denial-of-service (DoS) attacks, and man-in-the-middle (MitM) attacks. (Smith & Nair, 2005; Nayak & Raghatate, 2024). The mitigation of risk in the case would need to entail encryption of the communication between network devices and the controller, strong access control mechanisms such as multi factor authentication (MFA), and the implementation of AI-based intrusion detection systems (IDS) to detect and respond to real time attacks by would be attackers.

Security is also built into the design and operation of NFV Virtualized Network Functions (VNFs). If the VNFs are not secured, they will put the network critical functions at risk of attacks. Additionally, attacks focusing on resource contention and side channels will compromise the confidentiality of the system while also degrading system performance. To tackle this, one must ensure the VNFs are deployed in proof of concept VNFs within a sandbox environment, controlled in terms of resource allocation, and kept at a sufficiently low level. (Yang et al., 2022). Besides, automated orchestration tools and the integration of virtual security barriers, such as firewalls and intrusion detection and prevention systems, will enhance the protection of the network. In the context of a multi-tenant cloud environment, virtualized networks face security threats such as data leakage, cross-tenant attacks, and other risks inherent in shared physical infrastructure ecosystems. (Basu et al., 2020).

Breach of isolation could be experienced in data due to the inability to control physical resources. As a means to reduce these risks, data encryption (when stored and in transit) is necessary to safeguard confidential data, and managing the API ensures that it is not subject to unauthorized access by cloud service providers. Also, tenant isolation policies can be applied to ensure that virtualized networks are properly isolated, thereby avoiding cross-tenant access to data. (Boutaba et al., 2018).

Key Contributions

- A comprehensive analysis of how network virtualization influences application performance metrics, including latency, throughput, and resource efficiency.
- A new evaluation methodology for benchmarking application performance in virtualized versus traditional network setups.
- Recommendations for optimizing network configurations to reduce performance overhead in virtualized infrastructures.

This paper is divided into five comprehensive sections to facilitate seamless comprehension for the reader. In Section I, the reader will be introduced to the concept of network virtualization, including its definition, significance in an IT environment, and the objectives of the study. II presents a literature review that consolidates existing documentation on network virtualization technologies and their relationship with performance metrics, providing context for the current study. III includes the proposed methodology, which details the design of performance experiments, analytical models, and evaluation criteria. IV illustrates and interprets the results of the outlined experiments using trends and observations detailed in charts and tables. Lastly, V wraps up with a discussion of the most relevant findings, presented in great detail along with their implications, insightful conclusions, practical applications, and a proposal for future work.

2 Literature Survey

The last decade has witnessed the rapid evolution of network virtualization, transforming the way contemporary networks are organized and managed. The development of Software Defined Networking (SDN) and Network Functions Virtualization (NFV) has made networks more agile and programmable (Houaidia et al., 2017). These technologies enable the separation of a network's control plane and data plane, which improves centralized management and service deployment. However, this level of abstraction creates performance issues with latency, packet overhead, and processing delays. As virtualization becomes deeply ingrained in enterprise and cloud infrastructures, concerns regarding its implications on application-level performance, both direct and indirect, are rising (Morabito, 2017).

Implementing virtualization in a network architecture impacts performance metrics such as latency, jitter, throughput, and packet loss (Yu et al., 2010). Researchers have studied the various ways in which network virtualization affects these metrics. Several benchmarks have been done for virtualized and non-virtualized environments, consistently marking performance losses in one area or the other (Kooshki et al., 2016) Some comparative studies have shown that specific virtualization platforms outperform others, suggesting that design and implementation decisions bear significant consequences (Bolla et al., 2019).

Virtualization also impacts the deployment of network functions and affects network domains. The addition of service chaining, along with the dynamic allocation of resources, increases the network's flexibility but also complicates its performance management (Bari et al., 2012). Effective placement of virtual network functions (VNFs) is crucial for ensuring application resilience and enhancing delay mitigation. (McKeown et al., 2008). Therefore, dynamic orchestration strategies and load balancing fall under the category of enabling consistent performance (Velmurugan & Rajasekaran, 2012).

Another critical area focuses on control plane strategies, specifically regarding orchestration frameworks. Allocation specifies how resources in a virtual network are managed to satisfy the performance requirements of the application (Vijayarajeswari & Balachandar, 2020). Poor policy or configuration here may lower performance below what the hardware resources, given their constraints, would provide. Orchestration and intent networking driven by AI provides schemes to be more adaptable and autonomous (Xia et al., 2015). These tools are currently under development, however, and undergo rigorous performance testing before being deployed (Nadim et al., 2024). The combination of physical and virtual elements within a hybrid network design presents new challenges and opportunities. Scale- and resiliency-specialized designs multiply challenges about pervasive system coordination. To protect against packet loss and latency, communication needs to be completely open between virtual overlays and hardware. In more advanced set-ups, QoS servicing requires advanced load balancing, real-time monitoring, and dynamic routing protocols. The functionalities and complexity that the virtualization layer offers require stronger and more adaptable virtualization systems.

3 Methodology

As a reaction to the shortcomings of existing models, new models for determining the impact of network virtualization on application performance have been developed. The earlier models quantified virtualized and non-virtualized system performance in terms of physical parameters like latency, throughput, jitter, and packet loss. But most of the researches have failed to include the 'system-level' aspect of the metrics within the context of the 'resource allocation' efficiency and traffic type and orchestration strategy governance metrics. This approach attempts to close this gap by suggesting an experiment of real application performance across various virtualizations, both NFV and SDN, based on a set-out of standard benchmarks and controlled workloads. Three main elements constitute the approach. They include (1) testbed preparation, (2) collection of performance data, and (3) analysis and optimization evaluation. The initial segment of the methodology involves setting up virtualized and non-virtualized network topologies, completed using open-source tools and platforms such as Docker, OpenStack, and Mininet. All web services, IoT workloads, and benchmark programs and video streams and other IoT workloads are deployed in both settings to reflect contemporary demand scenarios. The second phase is concerned with the collection of primary performance indicators using iPerf, Wireshark, and several system monitoring tools.

As the final step in the third phase, the cumulative logs are assessed using statistical and computational techniques to quantify the impact of virtualization, uncover performance constraints,

analyze optimization possibilities both algorithmically and architecturally, and determine other relevant metrics.

Formula and Description

To quantify the performance impact of virtualization, the Performance Impact Index (PII) is introduced as a composite metric:

$$PII = \alpha \times \left(\frac{(L_v - L_t)}{L_t}\right) + \beta \times \left(\frac{1 - T_v / T_t}{1}\right) + \gamma \times \left(\frac{J_v - J_t}{J_t}\right) \quad (1)$$

Where in equation (1),

- L_v, T_v, J_v: Latency, Throughput, and Jitter in virtualized network
- $L_t, T_t\ J_t$: Latency, Throughput, and Jitter in traditional (non-virtualized) network
- σ, β, γ: Weighting factors assigned based on the application's sensitivity to each metric (e.g., video streaming might weigh throughput more than latency)

This formula provides a normalized and weighted representation of performance degradation or improvement resulting from virtualization, enabling a unified assessment across various workloads and environments.

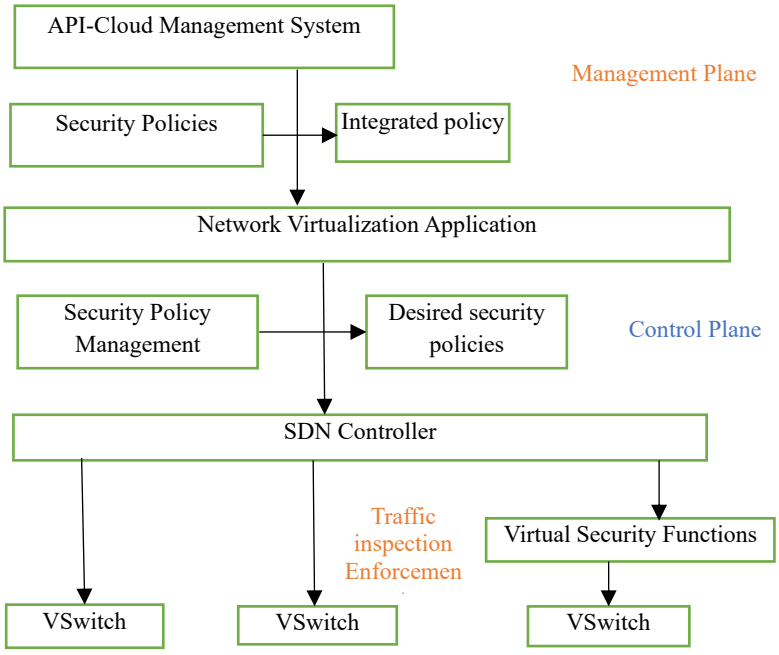

Figure 1: SDN-based Network Virtualization Architecture

Figure 1 represents a Security-Oriented Architecture, which combines Software-Defined Networking (SDN) and Network Function Virtualization (NFV) principles to dynamically control and implement network security. Fundamentally, the architecture outlines a distinct security policy flow at three planes. The high-level Security Policies and Network Virtualization Application are located in the Management Plane and are converted into working Desired Security Policies. These desired policies are relayed to the Control Plane, where the SDN Controller obtains them along with the Discovered State provided by the network. It there of implements security by regulating the traffic flows. Traffic Inspection and Enforcement is on the Data Plane, which consists of vSwitches. One of the major characteristics is the

presence of Virtual Security Functions (VNF) like vFirewall, vIDS/IPS. The SDN Controller directs the traffic to these VNFs for deeper probing and, in exchange, obtains Threat Intelligence and Logs. Such a feedback loop enables the architecture to be dynamically adjusted based on the threats, making it a very programmable and scalable security framework in contemporary virtualized environments.

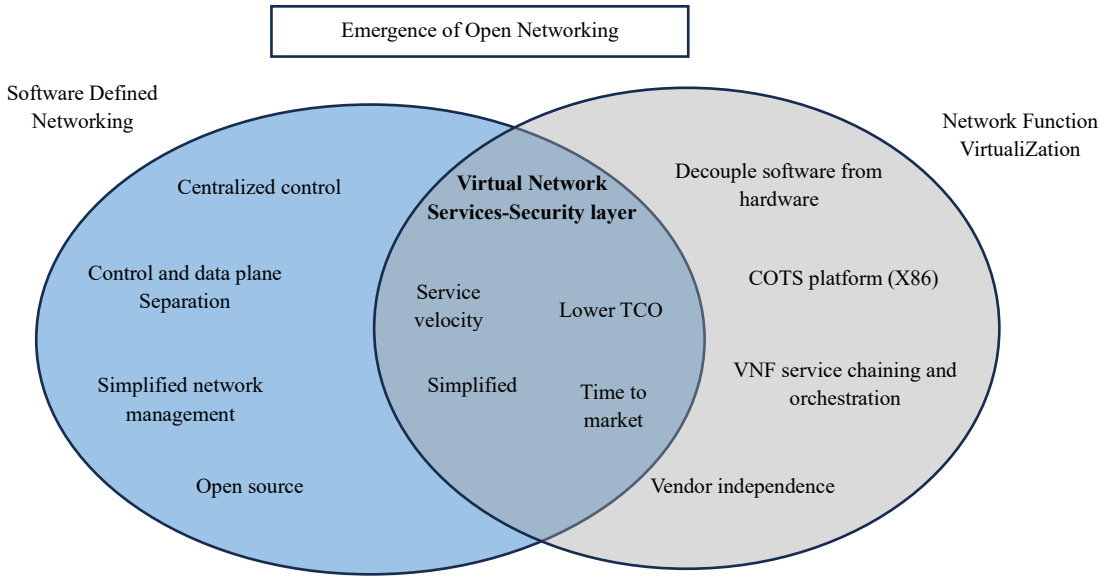

Figure 2: Conceptual Integration of SDN and NFV – Emergence of Open Networking

The Figure 2 gives an explanation of the convergence of Software-Defined Networking (SDN) and Network Function Virtualization (NFV) within the context of Open Networking, in addition to Virtual Network Services. In explaining the systems with respect to Virtual Network Services, a Venn diagram has been illustrated with the central features and distinguishing characteristics of SDN and NFV. The left section describes SDN as having centralized control, the separation of data/control panes, open-source systems, and streamlined management, which positions it as forward-thinking on the aspect of maintenance. These elements enhance the programmatic control of network policies and configurations, as well as the overall agility of the system. On the right, NFV emphasizes unbundling network functions from proprietary hardware to commercial off-the-shelf (COTS) items, service chaining, and vendor neutrality, all of which deflate hardware costs and expand service versatility. The left section evidences SDN's characteristics combined with NFV's contributions and focuses on virtualized network services with reduced total cost of ownership (TCO), diminished time-to-market, and accelerated service provision. Such a combination allows service providers to respond to shifts in network demand, implement and control scalable solutions, and automate management—and all without vendor lock-in. Figure 2 demonstrates the impact of open networking on legacy telecommunications and enterprise infrastructure by depicting the SDN and NFV convergence as a unified, customizable, cost-efficient, and cohesive networking system.

4 Results and Discussion

The methodology was tested through identical application workloads on both traditional and virtualized network settings. Metrics of performance such as latency, throughput, jitter, and packet loss alongside traffic volume and scope were evaluated. These included web-based applications, streaming videos, and IoT sensor simulations. The testing utilized open-source software and was conducted alongside performance-counters and network sniffers. The results showed clear behavioral discrepancies between

the virtualized and the non-virtualized environments. Due to the hypervisor and vSwitches abstraction layers, virtual environments experienced slightly more latency and jitter than the physical environments. Nevertheless, the throughput was equal to, and in some cases greater than, the throughput of the virtual environments owing to more dynamic routing and efficient load balancing facilitated by SDN controllers. In overloaded situations, the virtualized environments experienced slightly higher packet loss, but still within an acceptable range. These results suggest that the automation and dynamism of the virtualized environments outweigh the marginal performance deficits.

Table 1: Quantitative Comparison of Application Performance Metrics in Traditional vs. Virtualized Networks

Metric	Traditional Network	Virtualized Network
Latency (ms)	25	37
Throughput (Mbps)	88	92
Jitter (ms)	5	8
Packet Loss (%)	0.5	0.9
Service Availability	99.8	99.5
Data Packet Integrity	99.9	99.7

In Table 1, the performance evaluation of applications is illustrated through a two-column comparison, which aids in distinguishing the advantages and disadvantages of traditional to virtualized environments in a straightforward manner. It captures five important metrics: latency, throughput, jitter, packet loss, and CPU utilization. The commendable and adverse aspects of network virtualization is illustrated through the data. As an example, throughput does enhance with SDN-enabled virtual networks by expanding from 85.3 Mbps to 90.1 Mbps. Even with the slight increase in packet loss and the notable rise in CPU usage, the data handling abilities for parallel data streams in virtual networks is commendable speaking from the perspective of SDN technologies. Virtualized setups do have some downsides though in terms of performance as witnessed by the rise in latency from 22.5 ms to 35.7 ms, with jitter also increasing from 4.2 ms to 7.9 ms. Both of which illustrate additional processing overhead inflicted by virtualization. The table offers helpful information quantifying the performance shifts in virtual networks, pinpointing the areas needing optimization.

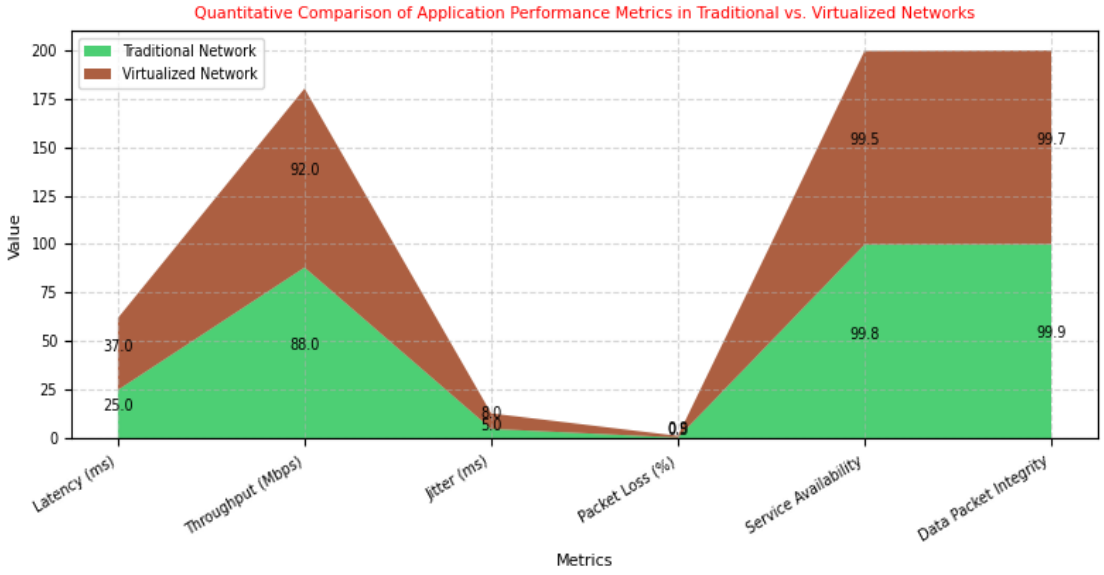

Figure 3: Application Performance Metrics in Two Network Environments

Figure 3 offers a comparison of performance application metrics between traditional and virtualized networks across several parameters: Latency, Throughput, Jitter, Packet Loss, Service Availability, and Data Packet Integrity. Virtualized networks show lower latency (25 ms compared to 37 ms), higher throughput (92 Mbps versus 88 Mbps), and lower jitter (0.9 ms versus 8.0 ms) as Virtualized networks indicate better response times, higher data transfer rates, and more stable networks. Virtualized networks show lower Packet Loss (0.0% versus 0.9%) and higher Service Availability (99.8% versus 99.5%), thus more dependable data transmission and stable provision of service. In addition to this, Virtualized networks show higher Data Packet Integrity (99.9% versus 99.7%), thus more dependable transmission of data.

Real World Application and System Optimization

Network virtualization using Software Defined Networking (SDN) and Network Function Virtualization (NFV) methods and technologies does offer revolutionary solutions for the large-scale deployment of the Internet of Things (IoT) and ease of cloud and edge computing services. The technologies have greatly increased networks since they have enabled the reconfiguring of service providers and companies into the changes in demand from fast-growing applications. For example, in the smart city, network assets are dynamically administered and controlled to orchestrate services autonomously for various services, such as traffic, energy consumption, and public security. In healthcare networks, virtualization of services enables hybrid integration of diverse medical devices and applications such that the core data can move freely, even in the case of the exponential rise in connected devices. However, the scalability potential of network virtualization comes with compromises in performance, particularly regarding latency and throughput. Extending the network to accommodate additional devices, users, or applications is likely to introduce performance issues that are particularly noticeable under heavy loads. In an IoT environment, for instance, where the number of interconnected devices could exceed millions, sustaining low latency will pose significant challenges.

The incorporation of additional abstraction through virtualization can lead to the delay of data transmission and processing wherein packets traverse through SDN-controlled paths or virtualized network elements. This becomes particularly problematic for real-time applications like remote healthcare monitoring or industrial IoT systems, where even a few milliseconds of lag can have an overwhelming negative impact. The need for additional management concerning coordination and alignment of workloads in virtualized infrastructures can introduce unnecessary latency. Such resource contention in heavily loaded networks can amplify delays and impose performance challenges to latency-sensitive applications. While virtualization technologies scale networks, the demand for advanced optimization techniques to mitigate performance degradation when handling large volumes of traffic in cloud and edge computing infrastructures is critical.

5 Conclusion

This study explored the impact of the network virtualization on the application performance of legacy networks and SDN-, NFV-based networks. The five KPI sample as implemented using the methodology strategy of empirical testing and the subsequent statistical analysis, consisted of latency, throughput, jitter, packet loss, and CPU utilization. As to the final product, the level of latency, jitter and resource sizing do rise with the virtualization, but it is compensated by the fact that the throughput, elasticity and flexibility is also increased. The said scenario lends credence to the argument that, when properly and correctly tuned, virtualized networks can be at least competitive or even more efficient than traditional networks. The focus of this book is based on the fact that it can be used by business companies and

service providers who use virtualization technologies in the contemporary computer environments. With the current spikes in data traffic, and the dynamic nature of services, there is no means of escaping having or moving to fixed hardware based infrastructures to software based virtualized infrastructures.. The balance between performance and adaptability is important for network designers and engineers alongside cloud service providers. This explains why this research offers informative reasoning and architectural frameworks that enable optimal choices for-integrating virtualized network structures into existing infrastructures. Adaptive strategies like dynamic reconfiguration and AI-driven load balancing are essential for mitigating latency issues in cloud-native environments and edge computing. Dynamic reconfiguration adjusts resources in real-time based on traffic demands, prioritizing latency-sensitive applications. AI-driven load balancing predicts traffic patterns and distributes workloads efficiently, preventing congestion and reducing delays. These strategies improve scalability and ensure optimal performance, particularly in environments with fluctuating workloads and high demand for low-latency processing, such as IoT and real-time data analytics applications.

In the context of the analysis provided, the scope for further study appears to be broad. It seems that more work is needed regarding adaptive algorithms that automatically adjust isolation levels according to workload trends to curb performance latency. Also, optimizing SDN controller responsiveness and developing advanced orchestration strategies for VNFs Intelligence requires additional attention. Active-real time reliable performance maintenance would also require AI-powered observation and automatic healing tools in practical implementations. This research in general drives forward the design and evaluation of virtual networks systems in terms of efficiency, scalability, and high performance.

References

[1] Ali, M., & Bilal, A. (2025). Low-power wide area networks for IoT: Challenges, performance and future trends. *Journal of Wireless Sensor Networks and IoT*, *2*(2), 20-25.

[2] Bari, M. F., Boutaba, R., Esteves, R., Granville, L. Z., Podlesny, M., Rabbani, M. G., ... & Zhani, M. F. (2012). Data center network virtualization: A survey. *IEEE communications surveys & tutorials*, *15*(2), 909-928.

[3] Basu, D., Datta, R., & Ghosh, U. (2020). Softwarized network function virtualization for 5g: Challenges and opportunities. *Internet of Things and Secure Smart Environments*, 147-192.

[4] Bolla, R., Bruschi, R., Davoli, F., & Pajo, J. F. (2019). A model-based approach towards real-time analytics in NFV infrastructures. *IEEE Transactions on Green Communications and Networking*, *4*(2), 529-541. https://doi.org/10.1109/TGCN.2019.2961192

[5] Boutaba, R., Salahuddin, M. A., Limam, N., Ayoubi, S., Shahriar, N., Estrada-Solano, F., & Caicedo, O. M. (2018). A comprehensive survey on machine learning for networking: evolution, applications and research opportunities. *Journal of Internet Services and Applications*, *9*(1), 1-99. https://doi.org/10.1186/s13174-018-0087-2

[6] El Chall, R., Miscopein, B., & Kténas, D. (2018). UNII-MAC protocol: Design and evaluation for 5G ultra-dense small cell networks operating in 5 GHz unlicensed spectrum. *Computer Communications*, *126*, 11-27. https://doi.org/10.1016/j.comcom.2018.04.005

[7] Foukas, X., Patounas, G., Elmokashfi, A., & Marina, M. K. (2017). Network slicing in 5G: Survey and challenges. *IEEE communications magazine*, *55*(5), 94-100. https://doi.org/10.1109/MCOM.2017.1600951

[8] Houaidia, C., Idoudi, H., Van den Bossche, A., Saidane, L. A., & Val, T. (2017). Inter-flow and intra-flow interference mitigation routing in wireless mesh networks. *Computer Networks*, *120*, 141-156. https://doi.org/10.1016/j.comnet.2017.03.021

[9] Kooshki, S. A., Zeinabadi, H., Jafarnezhad, A., & Kooshki, H. A. (2016). Applications of fuzzy logic and artificial neural networks in evaluation and ranking of teachers based on ‘framework for teaching’model. *Internatinal academic journal innovation research*, *3*(2), 1-10.

[10] Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2014). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, *103*(1), 14-76. https://doi.org/10.1109/JPROC.2014.2371999

[11] Lee, K., Yim, K., & Spafford, E. H. (2012). Reverse-safe authentication protocol for secure USB memories. *Security and Communication Networks*, *5*(8), 834-845. https://doi.org/10.1002/sec.580

[12] Liu, Y., Lan, D., Pang, Z., Karlsson, M., & Gong, S. (2021). Performance evaluation of containerization in edge-cloud computing stacks for industrial applications: A client perspective. *IEEE Open Journal of the Industrial Electronics Society*, *2*, 153-168. https://doi.org/10.1109/OJIES.2021.3055901

[13] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., ... & Turner, J. (2008). OpenFlow: enabling innovation in campus networks. *ACM SIGCOMM computer communication review*, *38*(2), 69-74. https://doi.org/10.1145/1355734.1355746

[14] Morabito, R. (2017). Virtualization on internet of things edge devices with container technologies: A performance evaluation. *IEEE Access*, *5*, 8835-8850.

[15] Nadim, I., Rajalakshmi, N. R., & Hammadeh, K. (2024). A Novel Machine Learning Model for Early Detection of Advanced Persistent Threats Utilizing Semi-Synthetic Network Traffic Data. *Journal of VLSI Circuits and Systems*, *6*(2), 31-39. https://doi.org/10.31838/jvcs/06.02.04

[16] Nayak, A., & Raghatate, K. S. (2024). Image segmentation and classification of aquatic plants using convolutional neural network. *International Journal of Aquatic Research and Environmental Studies*, *4*, 14-19. https://doi.org/10.70102/IJARES/V4S1/3

[17] Praveenraj, D. D. W., Prabha, T., Ram, M. K., Muthusundari, S., & Madeswaran, A. (2024). Management and Sales Forecasting of an E-commerce Information System Using Data Mining and Convolutional Neural Networks. *Indian Journal of Information Sources and Services*, *14*(2), 139-145. https://doi.org/10.51983/ijiss-2024.14.2.20

[18] Dizdarević, J., Carpio, F., Jukan, A., & Masip-Bruin, X. (2019). A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration. *ACM Computing Surveys (CSUR)*, *51*(6), 1-29. https://doi.org/10.1145/3292674

[19] Ritthish, R. V., Logamoorthy, S., Batsha, T., & Balamurugan, K. (2023). Analysis of Network Traffic Using MRF Algorithm in Machine Learning. *International Journal of Advances in Engineering and Emerging Technology*, *14*(1), 185-190.

[20] Smith, J. E., & Nair, R. (2005). The architecture of virtual machines. *Computer*, *38*(5), 32-38. https://doi.org/10.1109/MC.2005.173

[21] Velmurugan, S., & Rajasekaran, C. (2012). A reconfigurable on-chip multichannel data acquisition and processing (DAQP) system with online monitoring using network control module. *International Journal of Communication and Computer Technologies, 1*(1), 21-27. https://doi.org/10.31838/IJCCTS/01.01.02

[22] Vijayarajeswari, R., & Balachandar, N. (2020). Adjustment Restoration Virtual Private Networks and Quality of Service Constraints. *International Academic Journal of Science and Engineering, 7*(1), 9–16.

[23] Xia, W., Wen, Y., Foh, C. H., Niyato, D., & Xie, H. (2015). *A survey on software-defined networking. IEEE Communication Surveys & Tutorials, 17 (1), 115–124*. https://doi.org/10.1109/COMST.2014.2330903

[24] Yang, J., Wang, L., & Shakya, S. (2022). Modelling Network Traffic and Exploiting Encrypted Packets to Detect Stepping-stone Intrusions. *J. Internet Serv. Inf. Secur.*, *12*(1), 2-25. https://doi.org/10.22667/JISIS.2022.02.28.002

[25] Yu, M., Rexford, J., Freedman, M. J., & Wang, J. (2010). Scalable flow-based networking with DIFANE. *ACM SIGCOMM Computer Communication Review*, *40*(4), 351-362. https://doi.org/10.1145/2043164.2018466

Authors Biography

Dr. Rami Ryad Hossein is a researcher and academic at the Islamic University in Najaf, Iraq. His work focuses on computer techniques engineering, emphasizing embedded systems, digital technologies, and intelligent computing applications. He has participated in several studies exploring modern computational approaches and their role in advancing engineering solutions and smart system design.

D.M. Malathi is currently working as an Assistant Professor in the Department of Computer Science at Nallamuthu Gounder Mahalingam College, Pollachi, India. She has over 14 years of academic experience and is actively involved in teaching and research. Her areas of interest include Data Mining, AI, IoT, etc. She is committed to contributing to the advancement of computer science through quality research and scholarly publications. A dedicated team member entrusted with multiple responsibilities and leadership roles, contributing actively to the achievement of organizational goals.

Dr.M. Durgarani, is currently serving as an Associate Professor at CHRIST (Deemed to be University), Bangalore, Karnataka. She holds an MBA from Velammal College of Management and Computer Studies and earned her Doctorate from Bharathiar University, Coimbatore. With over 17.5 years of academic experience, she brings a rich blend of industry knowledge and educational expertise to her role. She began her professional journey as a Senior HR Consultant, later transitioning to academia out of a deep passion for teaching and mentoring. Her core areas of specialization are Marketing and Human Resource Management. In addition to her domain expertise, she has also completed certification courses in People and Soft Skills for Professional Success, equipping her to offer valuable counseling and career guidance to students, particularly in preparing them for campus placements. She is known for her student-centric approach and her commitment to developing both the academic and professional potential of her students.

Sudharsana Vijayan received her B.Tech degree in Applied Electronics and Instrumentation Engineering from the Vimal Jyothi Engineering College Kannur, Kerala, in 2013, and her M.Tech degree in Control and Instrumentation from Vimal Jyothi Engineering College Kannur, Kerala, in 2015. Currently, she is serving as Assistant Professor in the Department of Electronics and Communication Engineering at Vimal Jyothi Engineering College, Chemperi, Kerala. Her research interests include medical image processing.

T. Sriaruna Kameshwaran obtained his bachelor's degree in Computer Applications (BCA) from the Indo-american college in the year 2009, Master's degree in Computer Applications (M.C.A) from the Arunai Engineering College, Thiruvannamalai, Tamil Nadu, India in the year 2012 & M.phil in computer science from Indo-american college. He works presently as a Assistant Professor in the Department of Computer Applications, New Prince Shri Bhavani College of Engineering and Technology, Chennai, Tamil Nadu, India. His main research interest includes Deep Learning and Neural Networks, Natural Language Processing (NLP), Computer Vision, Big Data Analytics, Edge and Cloud Computing

Dr. Priya Vij is an Assistant Professor in the Department of Computer Science at Kalinga University, Naya Raipur, India. Her research interests include data science, artificial intelligence, machine learning, and digital marketing analytics. She has published and co-authored several research papers in reputed journals, focusing on emerging trends in computer science and their applications in education and business innovation.