ISSN 2581 – 3781

Available Online at www.ajcse.info
Asian Journal of Computer Science Engineering 2023;8(4)

REVIEW ARTICLE

Scalable Data Center Networking: Evaluating VXLAN EVPN as A Next-Generation Overlay Solution

Vaidehi Shah*
Independent Researcher

Received on: 15-10-2023; Revised on: 01-11-2023; Accepted on: 20-12-2023

***Abstract*—the rapid evolution of cloud computing, artificial intelligence, and distributed applications has transformed the operational landscape of modern data centers, demanding scalable, flexible, and resilient networking solutions. Traditional Data Center Network (DCN) architectures often hardware-bound and statically configured, struggle to accommodate the growing volume of east-west traffic and the need for automation and multitenancy. This paper presents an in-depth examination of VXLAN-EVPN architectures, detailing their operational principles, advantages, and implementation strategies in modern data centers. A comprehensive literature review is conducted to highlight current advancements, real-world use cases, and ongoing challenges, including scalability limits, verification inefficiencies, and energy consumption. Comparative analysis of recent works is provided to outline contributions, research gaps, and opportunities for further exploration. In order to satisfy future expectations, the study's conclusion highlights the significance of integrated, software-defined, and adaptable network systems. This work aims to guide network architects and researchers in designing secure, resilient, and next-generation data center networks aligned with emerging digital and cloud-native ecosystems.**

***Keywords*—VXLAN (Virtual Extensible LAN), EVPN (Ethernet VPN), Data Center Networking, Overlay Networks, Network Scalability.**

I. Introduction

The rapid expansion of cloud computing has transformed the digital landscape by enabling highly flexible, scalable, and on-demand telecommunication and IT services. These advancements are made possible through the implementation of large-scale data centers, which interconnect numerous hosts via high-speed networks. At the core of these infrastructures lies the Data Center Network (DCN), a critical component responsible for supporting seamless data exchange, service delivery, and efficient resource utilization [1]. For modern DCNs to offer transparent and continuous cloud operations, it must meet four essential requirements: auto-configuration, scalability, flexibility, and high availability, which includes resilience and fast failure recovery [2]. In response to these requirements, a range of DCN architectures has been proposed over the past decade. Although some designs, such as Portland, successfully address certain aspects like simplified configuration and availability, they typically fall short of delivering all four goals concurrently. This shortfall is particularly evident as data center demands grow, driven by rising data volumes and diverse application needs. These limitations highlight a key challenge: traditional DCNs, which rely heavily on static, hardware-based designs, are becoming increasingly inadequate in dynamic and data-intensive environments [3].

As these challenges intensify, there is a growing need to decouple DCN functionalities from rigid hardware constraints. This has led to the adoption of virtualization within modern data center environments, enabling network functions to operate across physical, hybrid, and multi-cloud infrastructures [4]. By abstracting network services from physical components, virtualization improves resource utilization, facilitates rapid deployment, and enhances operational agility. However, realizing these benefits at scale requires robust overlay solutions that can support multi-tenancy, fault tolerance, and high-performance routing. One of the most promising technologies in this domain is the VXLAN (Virtual Extensible LAN) in combination with EVPN (Ethernet VPN). Scalable Layer 2 overlays over Layer 3 networks are made possible by VXLAN, while EVPN serves as an efficient control plane that enhances mobility, convergence, and policy enforcement. Together, VXLAN EVPN addresses many of the core limitations of earlier overlay models, particularly in terms of scalability, automation, and interoperability, making it a viable solution for next-generation data centers. This paper examines the role of VXLAN EVPN as a next-generation overlay solution, analyzing its architecture, capabilities, and performance in comparison to legacy and contemporary alternatives. The discussion is supported by technical insights and a comparative evaluation, aiming to guide network engineers and decision-makers in adopting scalable, resilient, and future-ready data center network designs.

A. Paper Organization

This paper is structured are: Section II outlines the concept of scalability in data centers, including scaling methods and the transition from traditional to modern architectures. Section III delves into the architecture and operational principles of VXLAN and EVPN, highlighting their benefits. Section IV reviews recent literature on network verification, identifying existing limitations and research gaps. Section V concludes with insights and future research directions aimed at advancing scalable and adaptive next-generation DCNs.

II. Overview of Scalability in Data Center Networking

The capacity of a data center to operate efficiently as the quantity and size of its internal components, such as servers, increase is known as data center scalability. It is clear that data rise in the future, consequently, the data center must include a scaling function to effectively align with customer demand. The primary advantage of data center scalability shows in Table I, its capacity to enable a corporation to swiftly adjust its resources to fulfil its customers' precise needs [5]. Additionally, it offers the benefits of high density, energy efficiency, and cost savings throughout the lifespan of data center investments. To ensure the scalability of a data center, firms must choose a site that can be easily expanded in the future [6]. To thrive in a competitive environment, firms must adopt a strategic approach to data center implementation and scalability. The NETFORCHOICE data center facilitates the ability to adapt to evolving business and consumer requirements, adhere to stringent laws, and mitigate emerging risks. The hyper-converged infrastructure with scaling technologies is the premier purpose-built infrastructure for hosting contemporary virtualized data centers and hybrid clouds.

TABLE I. DATA CENTER SCALING METHODS

Method	Description	Pros	Cons
Adding more servers	Also known as scaling out or horizontal scaling, this involves adding more physical or virtual machines to the data center architecture.	✓ Can support and distribute more workloads ✓ Eliminates hardware constraints	✓ Deployment and replication take time ✓ Requires more rack space ✓ Higher upfront and operational costs
Virtualization	Dividing physical hardware into multiple virtual machines (VMs) or virtual network functions (VNFs) to support more workloads per device.	✓ Supports faster provisioning ✓ Uses resources more efficiently ✓ Reduces scaling costs	✓ Transition can be expensive and disruptive ✓ Not supported by all hardware and software
Upgrading existing hardware	Also known as scaling up or vertical scaling, this involves adding more processors, memory, or storage to upgrade the capabilities of existing systems.	✓ Implementation is usually quick and non-disruptive ✓ More cost-effective than horizontal scaling ✓ Requires less power and rack space	✓ Scalability limited by server hardware constraints ✓ Increases reliance on legacy systems
Using cloud services	Moving some or all workloads to the cloud, where resources can be added or removed on-demand to meet scaling requirements.	✓ Allows on-demand or automatic scaling ✓ Better support for new and emerging technologies ✓ Reduces data center costs	✓ Migration is often extremely disruptive ✓ Auto-scaling can lead to ballooning monthly bills ✓ May not support legacy software

A. Evolution of Data Center Network Architectures

The rise of cloud computing, AI workloads, and hybrid settings has rendered traditional three-tier data centre network architectures insufficient. Modern applications demand scalable, low-latency, and east-west traffic-optimized designs that can integrate seamlessly with cloud platforms while ensuring performance, security, and regulatory compliance [7]. Challenges such as data sovereignty, high bandwidth needs, and zero-trust security, compounded by supply chain constraints and market disruptions, are pushing organizations toward automated, resilient, and API-driven network solutions aligned with cloud-native principles. A three-tier DCN architecture is shown in Figure 1 [8]. Unfortunately, even the best enterprise-class equipment may only be able to supply 50% of the total bandwidth from end to end.

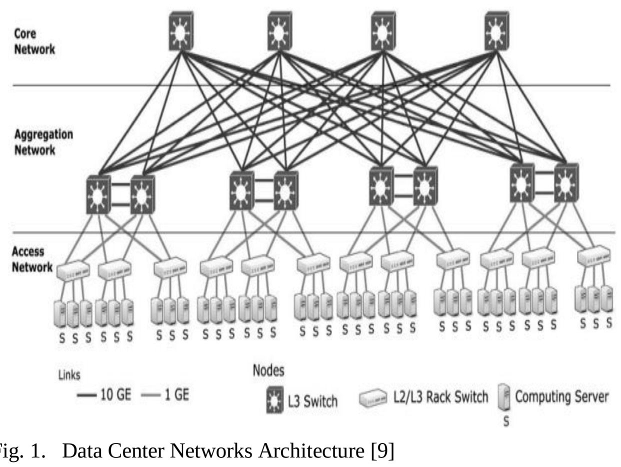

Fig. 1. Data Center Networks Architecture [9]

Key architectural approaches and implementation strategies that enable businesses to build resilient, scalable, and secure network infrastructures aligned with contemporary demands. From foundational architectural choices to advanced fabric designs, security implementations, and automation frameworks, they'll explore the essential building blocks of a modern data center network and provide practical guidance for organizations at any stage of their network transformation journey.

B. The Importance of Data Center Networking

Data center networking is crucial for establishing a stable, dependable, scalable, and secure network architecture. It ensures that infrastructure aligns with an organization's evolving communication needs while facilitating cloud computing and virtualization [10]. Moreover, business data center networking solutions improve operational consistency, automation, and security, which are essential for the successful delivery of data and application services. Data center networking is essential due to its:

- Consolidates resources and upholds operational uniformity by streamlining the integration of resources across cloud, on-premises, and edge environments, guaranteeing consistent rules and centralized control from a single interface.
- Facilitates network service delivery via job automation, workload balancing, and efficient network programming, hence allowing rapid adaptation to evolving requirements.
- Facilitates troubleshooting by offering an extensive overview of the network, hence simplifying the identification and resolution of problems promptly.
- Enhances data center security by shielding applications and data via integrated security measures such as IDS, IPS, and micro segmentation, hence mitigating cyber risks.

III. VXLAN AND EVPN: CONCEPTS AND ARCHITECTURE

A standards-based system called Ethernet VPN (EVPN) provides a virtual multipoint bridged connection between many domains via an IP and the IP/MPLS backbone network. Continuous, multi-tenant, flexible services that may be expanded on demand are made possible by EVPN. An extension of BGP called EVPN allows the network to simultaneously use L2 MAC and L3 IP data to enhance routing and switching choices [11]. Such control plane technologies employ Multiprotocol BGP (MP-BGP), which is intended for MAC and IP addresses at the endpoint distribution, where MAC addresses are considered routes. Devices operating as virtual tunnel endpoints (VTEPs) can share reachability data about their endpoints with one another thanks to EVPN. Businesses may readily add more core, distribution, and access layer devices to an expanding firm using an EVPN-VXLAN-based campus architecture, as shown in Figure 2, without having to rethink the architecture and buy a new set of equipment.

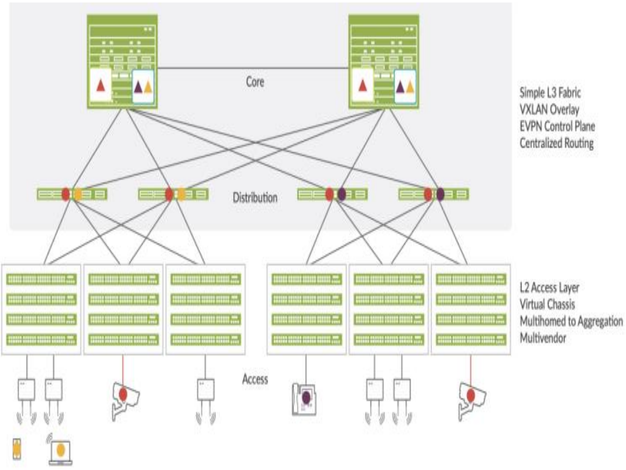

Fig. 2. EVPN-VXLAN-based Campus Architecture

In addition to support for Layer 2 and Layer 3 VPNs, businesses may employ a consistent set of policies and services across campuses. Campus network operators be able to create far bigger networks than would be possible with conventional Layer 2 Ethernet-based designs by combining an EVPN-VXLAN overlay with a Layer 3 IP-based underlay. Figure 3 illustrates how an IP fabric design with an EVPN-VXLAN overlay is often used in the most recent large-scale data centres.

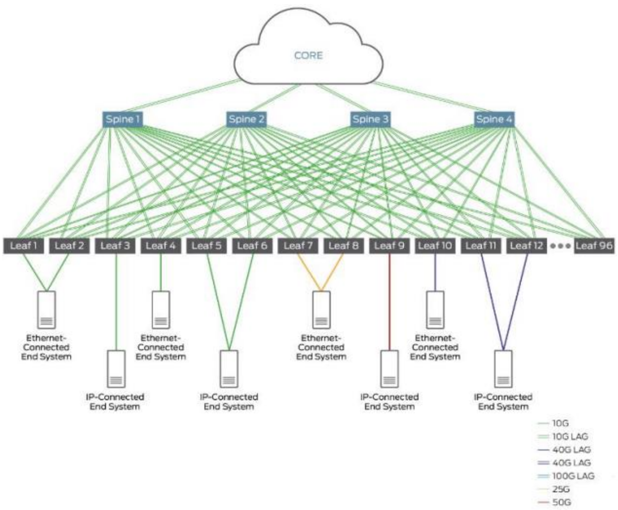

Fig. 3. Data Center Fabric Architecture

The two-tier spine-and-leaf architecture of the IP fabric, which is suited for large-scale environments, enables to collapse of traditional networking layers. This highly interconnected Layer 3 network may be readily scaled horizontally as needed and acts as an underlay to provide high resilience and low latency across the network. The EVPN-VXLAN overlay, which is placed on top of the IP fabric, allows for extending and connecting the Layer 2 data centre domains and place endpoints (such as servers or virtual machines) anywhere in the network, even between data centres. Some of the benefits offered by VXLAN EVPN systems include the following.

- Standards-based control plane (BGP) and standards-based overlay (VXLAN)
- Software-Defined Networking (SDN) facilitation
- The control plane (BGP) distributes Layer 2 MAC and Layer 3 IP information.
- Combining virtual and physical networks with hybrid overlays
- Optimizing Forwarding in the Overlay using Integrated Routing/Bridging (IRB)
- Facilitation of Software-Defined-Networking (SDN)
- Making decisions about forwarding based on a scalable control plane reduces flooding.
- Leverages Layer 3 ECMP in the underlay for complete link forwarding.
- The overlay's namespace is noticeably larger (16M segments).

A. *Virtual Extensible Lan (VXLAN) Overlay*

A network overlay is a technique used in contemporary data centres to virtualize a network and create an architecture that is more flexible than a network that is inherently static. Instead, it is important to spend some time understanding why typical networks are so static before getting into the specifics of how overlays work, the challenges they encounter, and how to get beyond these obstacles. The first message sent by an application is received by an overlay, which wraps it and the destination before sending it over the network. The communication is decapsulated and delivered as desired once it reaches its final destination. The sites are located in the encapsulation, which keeps the identity and location apart, but the initial message contains the identities of the communication devices (applications). This encapsulation and decapsulation process must be completed very rapidly and effectively since it is done on a per-packet basis. The architecture of VXLAN Overlay is shown in Figure 4.

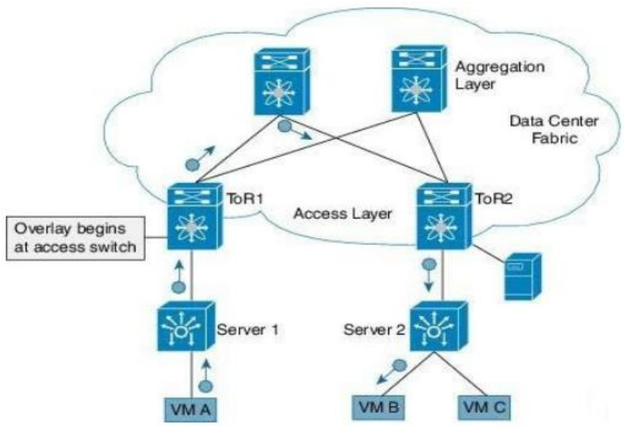

Fig. 4. VXLAN Overlay [12]

At present, between 60% and 70% of all application workloads are virtualized, according to market data; yet, more than 80% of servers are not running a hypervisor. It goes without saying that each data centre has a different combination of servers running both virtualized and non-virtualized applications. This combination should be covered by all of the data center's network solutions. The network problems that old VLAN technology produced in data centres were addressed by the IETF-recommended Virtual Extensible LAN (VXLAN) standard. The VXLAN standard provides the improved scalability of Layer 2 segmentation and variable workload allocation required by current application demands.

IV. LITERATURE REVIEW

There have been few studies published regarding the security aspect in a VXLAN environment. Most studies handle security in networking and focus on the security of Virtual machines (VM). Some notable papers in the field of data center network are as:

You et al. (2022) network overlay East-west and north-south traffic are managed by DCNs using firewall policies, policy-based routing, micro segmentation policies, and access control lists. Incremental verification techniques have been presented, however, they are inefficient or do not support specific network forwarding features. Test results demonstrate the accuracy and speed of incremental verification techniques. In terms of all-pair reachability, verifier outperforms current methods by up to 10x, for networks with 200 leaves, finishing the change-impact analysis in 15 seconds (4000 subnets and 16 million pairs) [13].

Salazar-Chacón and Marrone (2022) provide an Open Networking paradigm-based VXLAN proof-of-concept emulation and uses two approaches to validate the protocol's stated properties: The uncommon procedures known as Ethernet VPN (EVPN) and Lightweight Network Virtualization (LNV) provide scalable, affordable, and high-performing options for large-scale deployments [14].

Radoii and Rîncu (2022) in order to move towards a more centralized, integrated system, the costs of implementing and managing each device separately have decreased due to the improvement of dedicated networks as well as switching and routing capabilities. This article demonstrates the necessity of replacing the conventional network designs and protocols, including the VPC and Spanning Tree Protocol, by presenting the new network architecture and associated protocols for both the control plane and the data plane [15].

Lee and Lee (2021) suggest a scalable, secure Internet of Things (SSI) network architecture that shields IoT devices from security threats while preserving their processing power. VPN on Layer 2 Data connection frame encryption is offered by SSI, which is less demanding than TCP/IP VPN. Scalable layer 2 VPNs are offered by L2TP and VXLAN, whereas MACsec encrypts frames. SSI decreases CPU utilization by 31.6% and enhances network performance by 30% when compared to IoT networks using OpenVPN [16].

Baziana and Drainakis (2021) suggested MAC algorithm supports a variety of traffic kinds while avoiding channel collisions and achieving high effectiveness. To ascertain the scalability and performance bounds of the suggested MAC protocol, examine its performance under a variety of server populations per cluster. The simulation study shows that the proposed DCN architecture with the MAC protocol performs well for a range of server populations, with almost 100% bandwidth exploitation, low latency, low dropping rate, and high throughput [17].

Eltraify, Mohamed and Elmirghani (2020) proposes a Mixed Integer Linear Programming (MILP) model to maximize the deployment of virtual machines (VMs) throughout a data centre architecture built on the energy-efficient WDM-TDM AWGR PON. The use of virtual machines (VMs) and their requirements affect the optimal number of servers used in the data centre when reducing power consumption and facilitating more efficient server utilization are taken into account. For a maximum of 20 virtual machines (VMs) with varying compute and networking needs, two power consumption reduction goals were investigated. The findings show that when processing and networking power consumption are reduced, virtual machine allocation in the WDM-TDM AWGR PON may reduce networking power utilization by as much as 70% [18].

Despite significant advancements in data center networking (DCN), virtualization, and energy-efficient architectures, several research gaps remain. Existing solutions often focus on isolated aspects such as security, scalability, or energy efficiency, but lack an integrated approach that addresses all these dimensions simultaneously. Incremental verification methods, while faster, still fall short in supporting complex forwarding behaviors in heterogeneous network environments. Similarly, while emulation and virtualization strategies like VXLAN and LNV show promise, their real-world scalability and adaptability under dynamic workloads are yet to be fully explored. Furthermore, energy optimization models such as MILP are computationally intensive and not practical for large-scale or real-time deployments. These challenges and limitations are summarized in Table II, highlighting the need for unified, scalable, and adaptive frameworks that can ensure secure, high-performance, and energy-efficient operation in next-generation data center and IoT network infrastructures.

TABLE II. COMPARATIVE ANALYSIS OF RECENT RESEARCH ON DATA CENTER NETWORKS (DCNS), VIRTUALIZATION, AND OPTIMIZATION TECHNIQUES

Author	Focus On	Key Technologies	Contribution	Challenges	Future Study
You et al. (2022)	Verification of network policy in overlay DCNs	ACLs, Micro Segmentation, Policy-based Routing, Firewalls	Fast and accurate incremental verification algorithm for all-pair reachability	Incomplete support for certain forwarding behaviors in earlier methods	Extend support for more complex policies and forwarding behaviors
Salazar-Chacón and Marrone (2022)	Emulation of VXLAN networks using SDN	VXLAN, EVPN, Lightweight Network Virtualization (LNV)	Proof-of-concept for scalable, high-performance and low-cost network virtualization	Limited exploration of LNV in production-scale networks	Expand LNV-based emulation with dynamic and large-scale workloads
Radoii and Rîncu (2022)	Centralized routing and switching architecture	Integrated control/data plane, Modern alternatives to Spanning Tree & VPC	Redesigned network architecture with better integration and reduced cost	Complexity in replacing legacy systems	Migration strategies and hybrid models for gradual deployment

Lee and Lee (2021)	Secure, scalable IoT network infrastructure	Layer 2 VPN (L2TP, VXLAN), MACsec, SSI architecture	Improved security and performance for IoT networks, with low resource overhead	Balancing encryption overhead and resource constraints on devices	Broader deployment in heterogeneous IoT environments
Baziana and Drainakis (2021)	MAC protocol efficiency in DCNs	Custom MAC Protocol, Clustered Servers, Simulation Framework	High throughput, low delay, low drop rate under varied server loads	Performance under extreme traffic diversity	Real-time MAC adaptation for dynamic traffic patterns
Eltraify et al. (2020)	Energy-efficient VM placement in optical DCNs	MILP, WDM-TDM AWGR PON, VM profiling	Optimization of server use and network energy via VM placement	Computational overhead of MILP for large-scale data centers	Heuristic or AI-based models for scalable VM placement

V. CONCLUSION

Due to cloud technologies and multi-tenancy, network design has evolved fundamentally. Multi-data centers across locations are needed for business continuity. Enhancing old technologies and implementing new ones with plenty of additional features has become essential. This paper has explored the limitations of traditional network architectures and the potential of VXLAN-EVPN overlays to provide scalable, resilient, and flexible networking solutions. By decoupling network functions from physical infrastructure and enabling integrated Layer 2/Layer 3 communication, VXLAN-EVPN enhances operational agility and supports modern deployment paradigms such as hybrid and multi-cloud environments. However, despite these advantages, several limitations remain. Real-world implementations still face challenges in managing overlay complexity, ensuring efficient incremental verification, supporting heterogeneous legacy systems, and optimizing energy consumption. Additionally, large-scale dynamic workloads can introduce performance bottlenecks if not managed with adaptive and intelligent orchestration. Future research should focus on developing unified frameworks that combine network function virtualization, AI-driven traffic management, and policy-aware automation. Investigating lightweight security mechanisms and scalable verification models tailored for VXLAN-EVPN environments is also essential. Furthermore, energy-aware network designs and cross-layer optimization strategies can contribute to sustainable and cost-effective data center operations. Addressing these areas will be vital in realizing the full potential of next-generation data center networks that can handle the needs of the digital future.

REFERENCES

[1] J. Xiao, B. Wu, X. Jiang, A. Pattavina, H. Wen, and L. Zhang, "Scalable Data Center Network Architecture With Distributed Placement of Optical Switches and Racks," *J. Opt. Commun. Netw.*, vol. 6, no. 3, Mar. 2014, doi: 10.1364/JOCN.6.000270.

[2] R. Patel and R. Tandon, "Advancements in Data Center Engineering: Optimizing Thermal Management, HVAC Systems, and Structural Reliability," *Int. J. Res. Anal. Rev.*, vol. 8, no. 2, 2021.

[3] E. Rojas, J. Alvarez-Horcajo, I. Martinez-Yelmo, J. M. Arco, and M. Briso-Montiano, "Scalable and Reliable Data Center Networks by Combining Source Routing and Automatic Labelling," *Network*, vol. 1, no. 1, pp. 11–27, Jun. 2021, doi: 10.3390/network1010003.

[4] E. Rojas, G. Ibanez, J. M. Gimenez- Guzman, D. Rivera, and A. Azcorra, "Torii: multipath distributed Ethernet fabric protocol for data centres with zero- loss path repair," *Trans. Emerg. Telecommun. Technol.*, vol. 26, no. 2, pp. 179–194, Feb. 2015, doi: 10.1002/ett.2863.

[5] S. Al-Mashhadi, "A Scalable Data Center Network Design Strategies." Universiti Sains Malaysia, 2019. doi: 10.13140/RG.2.2.31202.38089.

[6] H. Qi, M. Shiraz, J. Liu, A. Gani, Z. A. Rahman, and T. A. Altameem, "Data Center Network Architecture in Cloud Computing: Review, Taxonomy, and Open Research Issues," *J. Zhejiang Univ. Sci. C*, vol. 15, no. 9, pp. 776–793, Sep. 2014, doi: 10.1631/jzus.C1400013.

[7] J. Shetty, Abhishek, and G. K. C, "Comprehensive Review of Datacenter Architecture Evolution," *Int. Res. J. Eng. Technol.*, vol. 7, no. 5, pp. 7420–7426, 2020.

[8] D. Kliazovich, P. Bouvry, and S. U. Khan, "GreenCloud: A Packet-level Simulator of Energy-Aware Cloud Computing Data Centers," *J. Supercomput.*, vol. 62, no. 3, pp. 1263–1283, Dec. 2012, doi: 10.1007/s11227-010-0504-1.

[9] K. Bilal *et al.*, "A Comparative Study Of Data Center Network Architectures," in *26th European Conference on Modelling and Simulation*, ECMS, May 2012, pp. 526–532. doi: 10.7148/2012-0526-0532.

[10] K. Kant, "Data Center Evolution," *Comput. Networks*, vol. 53, no. 17, pp. 2939–2965, Dec. 2009, doi: 10.1016/j.comnet.2009.10.004.

[11] T. Singh, V. Jain, and G. S. Babu, "VXLAN and EVPN for Data Center Network Transformation," in *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, IEEE, Jul. 2017, pp. 1–6. doi: 10.1109/ICCCNT.2017.8203947.

[12] A. S. George and A. S. H. George, "A Brief Overview of VXLAN EVPN," *Int. J. Innov. Res. Electr. Electron. Instrum. Control Eng.*, 2021.

[13] L. You, J. Zhang, Y. Jin, H. Tang, and X. Li, "Fast Configuration Change Impact Analysis for Network Overlay Data Center Networks," *IEEE/ACM Trans. Netw.*, vol. 30, no. 1, pp. 423–436, Feb. 2022, doi: 10.1109/TNET.2021.3114448.

[14] G. Salazar-Chacon and L. Marrone, "Open Networking for Modern Data Centers Infrastructures: VXLAN Proof-of-Concept Emulation using LNV and EVPN under Cumulus Linux," in *2022 IEEE Sixth Ecuador Technical Chapters Meeting (ETCM)*, IEEE, Oct. 2022, pp. 1–6. doi: 10.1109/ETCM56276.2022.9935681.

[15] A.-E. Radoi and C.-I. Rincu, "Integration of Data Center Network Technologies VxLAN, BGP, EVPN," in *2022 14th International Conference on Communications (COMM)*, IEEE, Jun. 2022, pp. 1–5. doi: 10.1109/COMM54429.2022.9817218.

[16] J. Lee and H. Lee, "Secure and Scalable IoT: An IoT Network Platform Based on Network Overlay and MAC Security," in *IFIP Advances in Information and Communication Technology*, 2021, pp. 287–301. doi: 10.1007/978-3-030-78120-0_19.

[17] P. Baziana and G. Drainakis, "A Scalable Optical Intra-Cluster Data Center Network with an Efficient WDMA protocol: Performance and Power Consumption Study," in *2021 30th Wireless and Optical Communications Conference, WOCC 2021*, 2021. doi: 10.1109/WOCC53213.2021.9603011.

[18] A. E. A. Eltraify, S. H. Mohamed, and J. M. H. Elmirghani, "VM Placement over WDM-TDM AWGR PON Based Data Centre Architecture," in *2020 22nd International Conference on Transparent Optical Networks (ICTON)*, IEEE, Jul. 2020, pp. 1–5. doi: 10.1109/ICTON51198.2020.9203100.