Comparing MPLS and next-generation routing: A conceptual model for performance, cost, and reliability tradeoffs

Jennifer Olatunde-Thorpe [1*], Stephen Ehilenomen Aifuwa [2], TheophilusOnyekachukwu Oshoba [3], Ejielo Ogbuefi [4], David Akokodaripon [5]
[1] Union Bank of Nigeria, Lagos, Nigeria
[2-3] Independent Researcher, Nigeria
[4] Company: NovantaInc, Bedford, MA, USA
[5] Take Blip, Brazil

* Corresponding Author: **Jennifer Olatunde-Thorpe**

Article Info

P-ISSN: 3051-3502
E-ISSN: 3051-3510
Volume: 03
Issue: 01
January - June 2022
Received: 19-02-2022
Accepted: 18-03-2022
Published: 16-04-2022
Page No: 110-119

Abstract
The evolution of enterprise networking has been shaped by the need to balance performance, cost, and reliability in increasingly complex digital environments. Multiprotocol Label Switching (MPLS) has long served as a cornerstone of high-performance, carrier-grade infrastructures, offering deterministic routing, quality of service (QoS), and strong reliability guarantees through service-level agreements (SLAs). However, with the rise of cloud adoption, distributed enterprises, and remote workforces, next-generation routing solutions—such as Software-Defined Wide Area Networking (SD-WAN), Segment Routing, and intent-based networking—have emerged as cost-effective, flexible alternatives. These technologies leverage internet broadband, cloud-native architectures, and adaptive routing algorithms to deliver scalable and agile connectivity. This develops a conceptual model for comparing MPLS and next-generation routing across three core dimensions: perf, cost, and reliability. MPLS excels in predictable latency, low jitter, and guaranteed packet delivery, but its benefits are coupled with high operational and capital costs. Conversely, next-generation routing platforms provide dynamic optimization, bandwidth efficiency, and lower costs, yet their reliance on public or shared infrastructure introduces variable reliability and new security challenges. The proposed model highlights tradeoff zones where organizations must prioritize based on operational context—for example, financial institutions may prioritize MPLS for mission-critical applications, while distributed enterprises may adopt SD-WAN for agility and cost savings. Beyond technical performance, the analysis also considers governance, compliance, and security implications, recognizing that routing decisions intersect with broader enterprise risk management. Future directions point to the role of artificial intelligence, machine learning, and digital twin simulations in predicting network behavior and optimizing tradeoffs in real time. By framing the comparison within a structured conceptual model, this study provides enterprises with a decision-making framework to align networking strategies with evolving demands for performance, cost efficiency, and resilience in the digital era.

DOI: https://doi.org/10.54660/IJMER.2022.3.1.110-119

Keywords: MPLS, Next-Generation Routing, Conceptual Model, Performance, Cost, Reliability Tradeoffs

1. Introduction

The digital era has transformed the landscape of enterprise and service provider networking, introducing new demands for agility, scalability, and resilience (Awe *et al*., 2017; Oni *et al*., 2018). Enterprises today rely on distributed architectures to support global operations, cloud-native applications, remote workforces, and latency-sensitive services such as real-time collaboration,

video
streaming, and industrial IoT. In parallel, service providers face the challenge of delivering secure, high-performance connectivity across heterogeneous environments while managing growing traffic volumes and increasingly dynamic user requirements (Awe, 2017; Ogundipe *et al*., 2019). These pressures have elevated networking from a back-end utility to a critical enabler of digital business strategies.

Within this evolving context, Multiprotocol Label Switching (MPLS) has played a foundational role in enterprise and carrier-grade networks for more than two decades (Awe *et al*., 2017; Akpan *et al*., 2017). MPLS revolutionized packet forwarding by introducing label-based switching, enabling predictable latency, reduced jitter, and traffic engineering capabilities essential for mission-critical workloads (ONYEKACHI *et al*., 2020). It quickly became the standard for delivering virtual private networks (VPNs), Quality of Service (QoS) guarantees, and highly reliable connectivity backed by strong service-level agreements (SLAs). Even today, MPLS remains central to many organizations' networking strategies, especially in industries such as finance, healthcare, and government where reliability and deterministic performance are paramount (Adeshina *et al*., 2021; Ajayi and Akanji, 2021). However, its strengths come at a high cost. MPLS circuits are expensive to provision and scale, and their rigid architectures often lack the flexibility required for cloud-era networking (Awe, 2021; Ejibenam *et al*., 2021).

The limitations of MPLS have paved the way for next-generation routing technologies that aim to address the dual need for flexibility and cost efficiency. Among these, Software-Defined Wide Area Networking (SD-WAN) has gained significant traction, leveraging broadband internet and cloud-native architectures to deliver agile and cost-effective connectivity (Halliday, 2021; Katsina *et al*., 2021). Similarly, Segment Routing offers simplified traffic engineering and scalability, while intent-based networking introduces automation and intelligence to align network behavior with high-level business policies. These solutions prioritize programmability, dynamic optimization, and cloud integration, aligning better with contemporary digital transformation initiatives. However, while they lower costs and enhance adaptability, they also introduce new challenges related to reliability, security, and performance predictability, particularly when operating over shared public infrastructure (John and Oyeyemi, 2022; Oyeyemi, 2022).

Given these contrasting characteristics, enterprises are increasingly faced with strategic decisions about whether to retain MPLS, migrate to next-generation routing, or pursue hybrid approaches. To inform such decisions, there is a need for conceptual models that systematically compare MPLS and next-generation routing technologies (Oyeyemi, 2022; Ajayi, S.A.O. and Akanji). This aims to develop such a model, focusing on three critical dimensions: performance, cost, and reliability. Performance is central to ensuring business continuity and application quality of experience. Cost considerations, both capital and operational, determine the economic sustainability of network strategies. Reliability underpins trust in connectivity and is particularly vital for mission-critical applications. By framing the tradeoffs across these dimensions, the conceptual model provides organizations with a structured lens for evaluating networking options in light of their operational priorities and risk tolerances (Ajayi and Akanji, 2022; Onotole *et al*., 2022). Ultimately, this comparative framework seeks to advance understanding of the shifting balance between legacy and emerging technologies in enterprise networking. In doing so, it highlights not only the continued relevance of MPLS but also the opportunities and challenges presented by next-generation routing solutions. The goal is to enable informed decision-making that aligns technical performance with business objectives in an era defined by cloud integration, digital innovation, and resilience.

2. Methodology

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology was applied to ensure transparency, rigor, and reproducibility in developing the conceptual model comparing Multiprotocol Label Switching (MPLS) and next-generation routing technologies. A systematic literature search was conducted across databases including IEEE Xplore, ScienceDirect, SpringerLink, and ACM Digital Library, complemented by industry white papers and technical reports from network solution providers. The search strategy combined keywords such as "MPLS," "SD-WAN," "Segment Routing," "intent-based networking," "network performance," "cost efficiency," and "reliability in enterprise networks." Publications from 2005 - 2022 were included to capture both the legacy role of MPLS and the rise of next-generation routing frameworks.

Inclusion criteria focused on studies and reports that addressed at least one of the three core dimensions—performance, cost, or reliability—in relation to MPLS or next-generation routing technologies. Comparative analyses, case studies, simulation-based performance evaluations, and policy/architecture frameworks were considered eligible. Exclusion criteria removed sources that were purely descriptive without measurable or conceptual insights into tradeoffs, as well as duplicates, short editorials, and vendor-specific promotional materials without peer-reviewed evidence.

The screening process was conducted in two stages. In the first stage, titles and abstracts were reviewed to eliminate irrelevant publications. In the second stage, full-text assessments were performed to evaluate methodological rigor and relevance to the study's objectives. Data extraction captured performance metrics (e.g., latency, throughput, jitter), cost considerations (e.g., circuit provisioning, operational expenditure), and reliability measures (e.g., availability, failover, SLA adherence). Studies were also categorized based on their coverage of legacy MPLS deployments, emerging solutions such as SD-WAN and Segment Routing, or hybrid architectures integrating both.

The PRISMA workflow ensured a transparent filtering process, beginning with an initial pool of approximately 450 records, narrowing to 180 after abstract screening, and concluding with 85 full-text studies deemed highly relevant. These sources informed the conceptual model by identifying strengths, limitations, and contextual factors influencing enterprise decision-making. The methodology not only established an evidence base for analyzing tradeoffs but also enabled triangulation across academic, industrial, and applied perspectives. This systematic approach ensured that the resulting model reflects both technical insights and real-world applicability in enterprise and service provider environments.

2.1. Background and Context

The evolution of enterprise and service provider networking has been marked by successive waves of technological change, each responding to emerging operational demands and application requirements (Ogunyankinnu *et al*., 2022; Ajayi and Akanji, 2022). Multiprotocol Label Switching (MPLS) and the rise of next-generation routing paradigms illustrate this trajectory, as organizations seek to balance predictable performance, cost efficiency, and adaptive capabilities. Understanding the historical and contextual foundations of MPLS, as well as the emergence of software-defined and cloud-native approaches, provides a basis for evaluating tradeoffs and informing future deployment strategies.

Introduced in the late 1990s, MPLS was designed to overcome the limitations of traditional IP routing, particularly its reliance on destination-based forwarding and hop-by-hop decision-making. MPLS introduced the concept of deterministic paths by attaching short labels to packets, enabling routers to forward traffic along pre-defined Label-Switched Paths (LSPs). This mechanism provided a significant advancement in Quality of Service (QoS), allowing networks to prioritize latency-sensitive applications such as voice and video while ensuring bandwidth guarantees for mission-critical traffic.

Another major contribution of MPLS was in traffic engineering. By explicitly steering traffic flows, MPLS allowed operators to optimize the utilization of available network resources, avoiding congestion and ensuring resilience in the event of link failures (Alemayehu, 2019; Mayr *et al*., 2021). These features made MPLS the de facto standard for wide-area networking in enterprises and service providers, especially during the rapid expansion of global IP networks in the early 2000s. However, the architecture was hardware-centric and required significant investment in provisioning and maintenance, which later became a constraint as networks evolved toward greater flexibility and agility.

The limitations of MPLS in dynamic and cloud-driven environments catalyzed the development of next-generation routing paradigms. Software-Defined Networking (SDN) introduced centralized control through logically separated control and data planes, enabling programmable policies and network-wide visibility. SDN provided a means to dynamically allocate resources, simplify configuration, and accelerate service provisioning compared to the rigid and manual configurations typical of MPLS (Ogunyankinnu *et al*., 2022; Onibokun *et al*., 2022).

Cloud-native routing further advanced this paradigm by embedding routing intelligence directly into cloud infrastructures. Instead of relying solely on on-premise or carrier-based MPLS circuits, enterprises began leveraging cloud-based transit services and virtual routers, enabling seamless connectivity across hybrid and multi-cloud environments. This shift aligned with the growing enterprise need for agility, scalability, and integration with cloud applications.

A parallel trend is the emergence of AI-driven optimization in routing. Leveraging machine learning algorithms, these systems can predict traffic patterns, identify anomalies, and recommend or even autonomously implement routing changes. Such capabilities mark a departure from the static nature of MPLS paths, offering adaptive and predictive performance management (Leonard and Emmanuel, 2022). By integrating telemetry and real-time analytics, AI-driven routing enhances resilience and operational efficiency, addressing challenges such as traffic surges, cyberattacks, or sudden link degradations.

The transition from MPLS-dominated architectures to next-generation routing is not merely technological but also driven by fundamental shifts in enterprise demands. The rise of cloud adoption has redefined traffic patterns: rather than primarily being site-to-site, traffic increasingly flows between users and cloud-hosted services. This shift undermines the traditional hub-and-spoke model optimized by MPLS and necessitates more distributed, internet-based routing architectures.

At the same time, the proliferation of distributed users—including branch offices, mobile workforces, and edge devices—has created a need for flexible and scalable connectivity. MPLS, while reliable, was often criticized for its rigidity and high costs when extending services to multiple geographies. Next-generation solutions like SD-WAN emerged in response, providing cost-effective alternatives by leveraging broadband internet and integrating security services natively (James and Olivia, 2020; Asif and Ghanem, 2021).

The acceleration of remote work, particularly during and after the COVID-19 pandemic, amplified these requirements. Enterprises needed to deliver secure, low-latency access to cloud applications for globally dispersed employees. MPLS circuits, typically centralized and fixed, were poorly suited for such distributed architectures, while SD-WAN and cloud-native routing demonstrated their capacity to provide direct-to-cloud connectivity with integrated security (Ramdoss and Nainar, 2020; Shen and Brower, 2021).

Together, these dynamics reveal a broader pattern: networking has shifted from being primarily about deterministic performance guarantees toward a model that balances agility, resilience, and cost-effectiveness. MPLS remains valuable in scenarios requiring strict QoS and highly predictable service levels, but it struggles to address the scale, flexibility, and economic considerations of cloud-centric enterprises (Adekunle *et al*., 2021; Mohan *et al*., 2021). Next-generation routing paradigms, incorporating SDN, cloud-native approaches, and AI-driven intelligence, align more closely with contemporary business requirements, though they also introduce challenges around governance, interoperability, and reliability.

This contextual evolution frames the need for conceptual models that systematically compare MPLS and next-generation routing. By examining their tradeoffs in performance, cost, and reliability, enterprises and service providers can make informed decisions on whether to continue investing in MPLS, adopt next-generation solutions, or pursue hybrid architectures that integrate the strengths of both.

2.2. Conceptual Dimensions of Comparison

The debate between Multiprotocol Label Switching (MPLS) and next-generation routing paradigms hinges on a set of interrelated conceptual dimensions that determine their suitability for modern enterprise networking. Performance, cost, and reliability remain the most salient metrics guiding decision-making, as they reflect both the technical and economic viability of wide-area network (WAN) solutions as shown in figure 1(Frangopol *et al*., 2019; Lai *et al*., 2021). While MPLS has long been the gold standard for

deterministic service quality, the rise of next-generation routing approaches such as Software-Defined Wide Area Networking (SD-WAN), Segment Routing, and AI-driven optimization reframes the tradeoffs across these dimensions.
One of the defining strengths of MPLS lies in its ability to deliver highly predictable network performance. By establishing Label-Switched Paths (LSPs) with explicit traffic engineering capabilities, MPLS provides latency, jitter, and packet delivery guarantees that are critical for real-time applications like voice over IP (VoIP), video conferencing, and financial transactions. These guarantees are reinforced by service-level agreements (SLAs) from service providers, offering enterprises confidence in deterministic performance (Uriarte *et al*., 2019; Prasad and Bhavsar, 2020).

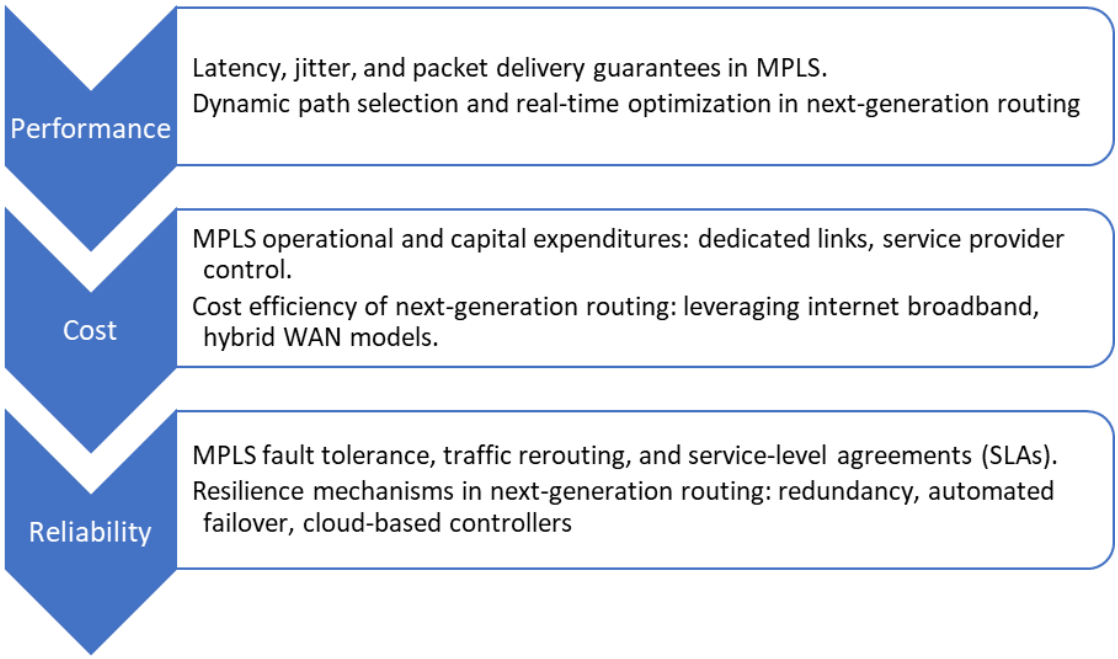

Fig 1: Conceptual Dimensions of Comparison

In contrast, next-generation routing prioritizes flexibility and adaptability. Through dynamic path selection and real-time optimization, SD-WAN and related technologies can route traffic over multiple links—including broadband internet, LTE, and MPLS—based on current conditions. Advanced controllers use telemetry and analytics to measure path quality and shift flows accordingly, ensuring that traffic receives the best available performance even in volatile environments. While such adaptability improves responsiveness to congestion or outages, it lacks the strict determinism of MPLS, as performance may fluctuate depending on the quality of underlying public internet links.
The tradeoff between deterministic and adaptive performance thus reflects differing philosophies. MPLS guarantees high performance under predefined constraints but struggles with scalability and agility. Next-generation routing thrives in distributed, cloud-centric contexts by continuously adapting to change, though enterprises must accept some variability in exchange for broader agility (Welsh and Benkhelifa, 2020; Woods *et al*., 2021).
Cost considerations represent a critical driver of the migration from MPLS to next-generation routing. MPLS networks involve significant operational and capital expenditures. Enterprises rely on dedicated circuits provisioned by service providers, often at premium costs, especially across international or geographically dispersed sites. In addition, provisioning MPLS links can be slow, requiring months to establish, thereby constraining business agility.
By comparison, next-generation routing models are designed for cost efficiency. SD-WAN, for example, leverages commodity broadband and mobile links alongside, or in place of, MPLS circuits. Hybrid WAN architectures allow enterprises to allocate high-priority traffic over MPLS while sending less sensitive data over public internet links, dramatically reducing bandwidth costs. Cloud-native routing approaches further minimize expenditure by replacing physical appliances with virtualized, subscription-based models that scale with demand (Haensge *et al*., 2021; Shah *et al*., 2021).
When considering total cost of ownership (TCO) over time, next-generation routing often proves more economical due to its reliance on widely available broadband and software-driven provisioning. However, MPLS's higher upfront and ongoing costs may be justified in industries where deterministic performance and carrier-grade SLAs outweigh financial savings. The cost dimension therefore highlights not only raw expenditure but also the alignment between financial investment and performance requirements.
Reliability has historically been a cornerstone of MPLS adoption. Carrier-managed MPLS networks are engineered for fault tolerance, with mechanisms such as fast reroute, traffic engineering, and redundant infrastructure minimizing downtime. Enterprises can rely on SLAs guaranteeing high availability and rapid recovery from failures, making MPLS especially appealing for mission-critical workloads in sectors like healthcare and finance.
Next-generation routing technologies approach reliability through different mechanisms. SD-WAN employs redundancy and automated failover, dynamically rerouting traffic over alternate links when degradation or failures are detected. Cloud-based controllers enhance this process by

providing centralized orchestration and real-time visibility, enabling rapid reconfiguration across distributed environments. Moreover, AI-driven systems can predict and mitigate disruptions before they occur, enhancing resilience beyond traditional MPLS capabilities.

Nonetheless, next-generation routing introduces a new risk assessment dynamic. By depending on public internet connectivity, these solutions are inherently exposed to potential variability in availability and security. While overlay protocols and encryption mitigate many risks, they cannot eliminate the fundamental unpredictability of the open internet. In contrast, MPLS, as a carrier-grade infrastructure, insulates traffic from such volatility by operating on private, dedicated circuits. This dichotomy underscores the reliability tradeoff: MPLS offers predictable stability, while next-generation routing provides resilience through adaptive, multi-path architectures that may carry more exposure to external risks.

Taken together, these conceptual dimensions reveal a nuanced comparison. MPLS excels in deterministic performance and carrier-grade reliability but comes at a premium cost and limited agility. Next-generation routing prioritizes adaptability, scalability, and cost efficiency, leveraging commodity infrastructure and real-time optimization to meet cloud-era demands, albeit with variable performance and greater dependence on the public internet (Raj and David, 2021; Thuraka, 2021).

The choice between MPLS and next-generation routing cannot be reduced to a binary. Instead, enterprises increasingly pursue hybrid strategies that combine MPLS for critical, latency-sensitive applications with SD-WAN or cloud-native solutions for cost-effective and scalable connectivity. This integrative approach leverages the deterministic strengths of MPLS where necessary while exploiting the adaptive and economical advantages of next-generation routing.

Ultimately, the conceptual model comparing MPLS and next-generation routing across performance, cost, and reliability provides a framework for evaluating tradeoffs in enterprise networking. The optimal solution depends on organizational priorities, risk tolerance, and long-term digital strategies, highlighting the continuing relevance of both paradigms in the evolving networking landscape.

2.3. Conceptual Model for Tradeoffs

The comparison between Multiprotocol Label Switching (MPLS) and next-generation routing paradigms cannot be understood in isolation from the tradeoffs they entail. Enterprises today operate in complex digital ecosystems where network demands span diverse priorities: ensuring predictable performance, optimizing cost, and maintaining high levels of reliability. These priorities often exist in tension, and decision-making requires a structured conceptual model that integrates these dimensions into a comparative framework. By positioning performance, cost, and reliability within a tradeoff matrix, organizations can visualize zones of value, risk, and opportunity, enabling context-specific choices aligned with strategic objectives (Bertoni, 2019; Kravchenko *et al*., 2020).

The proposed conceptual framework organizes the three core dimensions—performance, cost, and reliability—into an interdependent matrix. At one extreme, MPLS embodies the high-performance, high-reliability, but high-cost quadrant. It guarantees deterministic Quality of Service (QoS), latency control, and fault tolerance but requires substantial investment in dedicated circuits and managed services. At the other extreme, next-generation routing technologies—such as Software-Defined Wide Area Networking (SD-WAN), Segment Routing, and cloud-native orchestration—fall within the adaptive and cost-efficient quadrant, where performance and reliability are variable and context-dependent.

The comparative matrix highlights how each solution prioritizes one or more dimensions while accepting limitations in others. MPLS maximizes performance and reliability but incurs financial rigidity, whereas next-generation routing optimizes cost efficiency and agility but relies on less predictable infrastructures such as public broadband and multi-cloud environments. The framework thus offers a structured view of the tradeoffs enterprises must weigh, underscoring that no single solution optimally satisfies all three dimensions simultaneously.

The tradeoff matrix can be conceptualized as three distinct zones; This zone is dominated by MPLS, where deterministic performance metrics (low latency, low jitter, guaranteed packet delivery) and strong carrier-grade reliability come at the expense of higher capital and operational expenditures. Service-level agreements (SLAs) provide predictable assurance, making MPLS attractive to sectors where downtime or data loss carries critical financial or reputational consequences.Next-generation routing occupies a zone where adaptability and efficiency are prioritized. Dynamic path selection, real-time optimization, and software-based orchestration allow traffic to flexibly traverse multiple transport options. This reduces costs and enhances scalability, particularly in distributed and cloud-centric environments. However, reliability is variable, influenced by the volatility of public internet infrastructure and the maturity of overlay protocols.Many enterprises adopt a hybrid approach, positioned between the two extremes. Here, critical applications requiring guaranteed QoS remain on MPLS, while less sensitive or cloud-native workloads leverage next-generation routing. This balancing act represents a pragmatic tradeoff zone, where performance, cost, and reliability are optimized contextually rather than universally.

By visualizing these zones, the conceptual model emphasizes that tradeoff selection is not a binary decision but rather a spectrum of possibilities tailored to enterprise needs (Knaster and Leffingwell, 2020; Kazim and Koshiyama, 2020).

The utility of the conceptual model becomes clearer when applied to specific enterprise contexts.

Financial institutions represent a use case where MPLS often remains the preferred option. High-frequency trading platforms, payment networks, and regulatory compliance environments demand deterministic performance and carrier-grade reliability. Latency variations of even milliseconds can translate into financial losses or regulatory breaches. While MPLS imposes higher costs, the tradeoff is justified by the mission-critical nature of the workloads and the need for audited, SLA-backed services. For such enterprises, the conceptual model situates them firmly within the high-performance, high-reliability zone, with cost deprioritized in favor of stability and compliance.

Conversely, distributed startups and digital-native enterprises benefit more from next-generation routing solutions. These organizations prioritize agility, scalability, and cost-efficiency to support rapid growth and geographically dispersed teams. Cloud-based collaboration tools, customer

engagement platforms, and global e-commerce workloads are well served by SD-WAN or cloud-native routing, where real-time optimization can compensate for the variability of internet paths. While reliability is less deterministic than MPLS, startups tolerate such tradeoffs because cost savings and flexibility outweigh the risks. These enterprises align with the adaptive, cost-efficient zone, embracing variability as part of a broader innovation strategy.

A third category encompasses mid-sized enterprises undergoing digital transformation, where hybrid strategies become prominent. These organizations may maintain MPLS links for sensitive enterprise resource planning (ERP) systems or legacy workloads while migrating customer-facing or cloud-native applications onto next-generation routing frameworks. By straddling the balancing zone, they mitigate risks without fully sacrificing cost savings or agility (Falani *et al*., 2022).

The conceptual model underscores that evaluating MPLS versus next-generation routing requires moving beyond binary comparisons to a nuanced appreciation of tradeoffs. Enterprises must assess their workloads, risk tolerance, and financial strategies in light of the three dimensions. The visualization of tradeoff zones facilitates decision-making by highlighting not only the strengths of each technology but also the compromises involved (Filani *et al*., 2022).

As networking continues to evolve, the balancing act will become even more dynamic, with AI-driven optimization, federated orchestration, and policy-based governance further blurring the lines between deterministic and adaptive models. Enterprises that adopt frameworks for systematically evaluating tradeoffs will be better positioned to navigate these complexities and align network architectures with strategic priorities (Sobhy *et al*., 2021; Chukwuma-Eke *et al*., 2021).

The conceptual model for tradeoffs provides a structured lens through which MPLS and next-generation routing can be compared across performance, cost, and reliability. By mapping technologies into distinct tradeoff zones, the framework illustrates that enterprise decisions are shaped not by absolutes but by context-specific priorities. Financial institutions may gravitate toward MPLS for guaranteed reliability, startups may embrace next-generation routing for agility and efficiency, and many enterprises will occupy hybrid middle ground. Ultimately, this comparative matrix equips decision-makers with the tools to balance competing demands, fostering adaptive and resilient networking strategies in the digital era.

2.4. Policy, Governance, and Security Considerations

Networking decisions in enterprise and service provider contexts extend beyond performance, cost, and reliability. They are also shaped by complex layers of policy, governance, and security considerations that define the operational, regulatory, and trust environments in which technologies are deployed. As organizations increasingly operate across national borders, leverage distributed infrastructures, and adopt hybrid approaches that combine Multiprotocol Label Switching (MPLS) with next-generation routing solutions, governance challenges become central to sustainable adoption. Data sovereignty, cybersecurity, and oversight of hybrid deployments represent three critical axes of this dimension (Hummel *et al*., 2021; CULLEN *et al*., 2021).

One of the most pressing governance concerns relates to data sovereignty—the requirement that data remain within specific national or regional jurisdictions due to regulatory mandates. MPLS, as a private carrier-grade technology, traditionally offers greater control over traffic paths, enabling enterprises to ensure compliance with jurisdictional requirements. Service providers can configure MPLS circuits to guarantee that sensitive data flows remain within specified boundaries, a critical feature for highly regulated sectors such as banking, healthcare, and government operations.

By contrast, internet-based routing, as embodied in next-generation solutions such as SD-WAN and cloud-native overlays, introduces greater uncertainty. While traffic can be encrypted and directed through virtual tunnels, the underlying internet infrastructure may cross international borders unpredictably. This raises compliance challenges under frameworks such as the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA), or sector-specific mandates like HIPAA in healthcare. Ensuring regulatory adherence in these environments requires robust policy enforcement at the application and overlay layers, supplemented by careful auditing of provider practices.

Hybrid deployments exacerbate these issues, as enterprises must manage both MPLS circuits—aligned with traditional compliance models—and internet-based tunnels that traverse less deterministic infrastructures. The governance burden therefore shifts from the provider alone to a joint responsibility between enterprise and service provider, requiring transparent contracts, monitoring mechanisms, and multi-jurisdictional compliance strategies.

Security considerations in MPLS and next-generation routing differ significantly in both approach and risk profile. MPLS is often perceived as inherently more secure due to its isolation from the public internet. Traffic within MPLS circuits is logically separated and less exposed to common internet-based threats. However, MPLS does not inherently provide end-to-end encryption; enterprises must still implement additional layers of protection, particularly as data flows into cloud services.

In contrast, next-generation routing solutions emphasize encrypted tunnels, such as IPsec and SSL-based mechanisms, as a baseline security measure. These overlays integrate with modern paradigms such as zero-trust networking, where each user, device, and workload must authenticate continuously, regardless of its location on the network. This integration reduces reliance on implicit trust models and aligns with cloud-native security practices. However, the trust relationship shifts to the cloud and internet service providers, raising questions about visibility, control, and liability in case of breaches.

The complexity of managing encryption at scale, particularly in distributed and multi-cloud ecosystems, introduces new governance challenges (Cherukuri, 2019; Mohammad, 2021; Sakyi *et al*., 2022). For example, key management, certificate lifecycle monitoring, and policy synchronization across geographies become mission-critical. Additionally, encrypted traffic itself can obscure malicious activity, complicating intrusion detection and requiring enterprises to deploy advanced monitoring solutions capable of analyzing encrypted flows without violating privacy principles.

Thus, while next-generation routing offers a modernized approach to security through zero-trust frameworks and flexible encryption, its reliance on shared infrastructures increases the importance of governance agreements with

providers. Enterprises must establish clear accountability for patching, threat intelligence sharing, and breach reporting to maintain resilience.

Most enterprises are not making an immediate leap from MPLS to next-generation routing; instead, they adopt hybrid deployments where MPLS supports critical workloads while internet-based routing underpins less-sensitive or cloud-native applications. This transitional model, while pragmatic, introduces significant governance challenges.

First, policy harmonization across two distinct architectures is difficult. MPLS circuits often operate under strict SLAs and contractual obligations, whereas SD-WAN overlays provide flexibility but depend on multiple ISPs with varying service assurances. Coordinating governance across these environments requires sophisticated orchestration platforms that can translate enterprise-wide policies into enforceable rules across both infrastructures.

Second, visibility and monitoring are fragmented. MPLS providers typically supply detailed performance and compliance reports, while next-generation routing relies on telemetry from distributed edge devices and controllers. Enterprises must integrate these data sources into unified governance dashboards to ensure consistent oversight.

Third, security posture alignment becomes critical. MPLS networks may continue to depend on perimeter-based security models, whereas SD-WAN and cloud-native solutions embrace distributed zero-trust principles. Balancing these models without creating gaps or redundancies requires deliberate governance strategies that redefine responsibilities between enterprise IT teams, managed service providers, and cloud operators.

Finally, hybrid deployments highlight the risk of governance complexity itself. Managing parallel infrastructures increases operational overhead, regulatory risk, and dependency on diverse providers. Enterprises that fail to streamline governance mechanisms may find that hybrid deployments, while flexible, introduce more vulnerabilities than they resolve.

Policy, governance, and security considerations are fundamental to evaluating MPLS and next-generation routing technologies. MPLS offers deterministic control over data sovereignty and compliance, making it attractive to regulated sectors, but lacks inherent encryption and agility. Next-generation routing introduces flexibility, encrypted overlays, and alignment with zero-trust paradigms but raises challenges of jurisdictional compliance and provider trust. Hybrid deployments, while increasingly common, amplify governance complexity by requiring harmonization across divergent architectures.

Enterprises must therefore adopt comprehensive governance frameworks that address data sovereignty, establish clear provider accountability, and integrate consistent security practices across hybrid infrastructures (Singi *et al*., 2020; Janssen *et al*., 2020). Only by embedding policy and governance as core decision factors can organizations fully realize the benefits of network innovation while safeguarding trust, compliance, and resilience.

2.5. Future Directions

The future of enterprise networking is being shaped by the convergence of technological innovation, shifting enterprise demands, and evolving governance frameworks as shown in figure 2(Petricevic and Teece, 2019; Vahlne and Bhatti, 2019). Multiprotocol Label Switching (MPLS) and next-generation routing paradigms such as Software-Defined Wide Area Networking (SD-WAN), segment routing, and intent-based networking will coexist for some time, but their trajectories will diverge as enterprises adopt cloud-centric and AI-enabled models. Looking forward, three core themes define the evolution of these technologies: the integration of artificial intelligence (AI) and machine learning (ML) for predictive optimization, the role of multi-cloud strategies in driving next-generation architectures, and the long-term positioning of MPLS as a niche solution in high-assurance environments compared to the broad adoption of next-generation routing technologies (Sakyi *et al*., 2022).

One of the most promising developments lies in the application of AI and ML to routing optimization. Traditional MPLS networks rely on deterministic paths and traffic engineering rules configured by network operators. While this approach ensures predictable performance, it lacks adaptability to changing traffic patterns or emerging disruptions. In contrast, next-generation routing platforms increasingly embed AI/ML algorithms that analyze real-time telemetry from routers, applications, and endpoints (Alberti *et al*., 2019; Kansara, 2021). These systems can predict potential congestion, packet loss, or latency bottlenecks before they impact users, enabling preemptive rerouting.

For example, predictive path selection allows SD-WAN controllers to automatically switch traffic flows to alternate links based on early indicators of degradation, minimizing downtime and enhancing user experience. Similarly, ML-driven anomaly detection can strengthen cybersecurity by identifying unusual patterns that may signal Distributed Denial of Service (DDoS) attacks or data exfiltration attempts. Over time, AI-enabled optimization could evolve toward self-healing networks, where infrastructures autonomously adapt to dynamic demands without manual intervention.

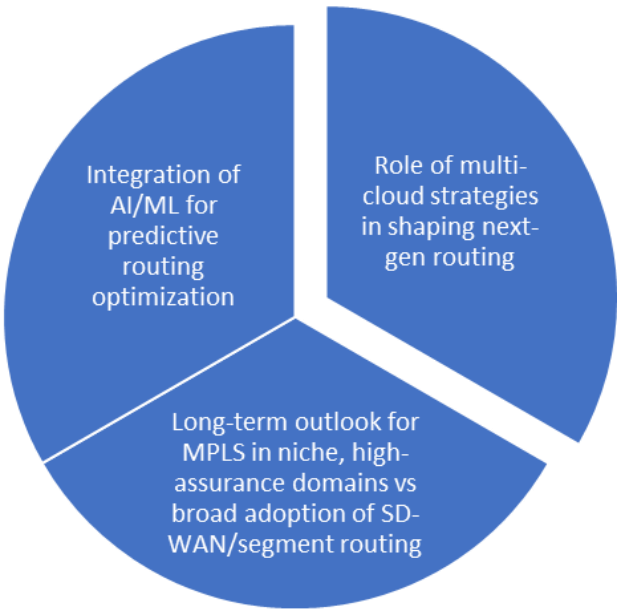

Fig 2: Future Directions

The integration of AI also offers enterprises greater operational efficiency, reducing reliance on human administrators for routine management. However, governance and transparency challenges remain, particularly around explainability in AI decision-making. As AI becomes central to routing optimization, enterprises must establish

accountability mechanisms to ensure these systems operate fairly, securely, and in compliance with regulations.

The rapid adoption of cloud computing is also reshaping the evolution of enterprise routing. Increasingly, organizations are adopting multi-cloud strategies, leveraging services from multiple providers (e.g., AWS, Azure, Google Cloud) to avoid vendor lock-in, optimize performance, and meet data sovereignty requirements. This shift requires routing infrastructures that are more flexible, application-aware, and capable of seamlessly interconnecting diverse environments. MPLS, while effective in private and controlled infrastructures, was not designed to support the fluidity of multi-cloud deployments. Its reliance on service provider-managed circuits limits agility when enterprises need to scale workloads across distributed cloud regions. By contrast, next-generation routing frameworks such as SD-WAN and segment routing are inherently cloud-centric. They can dynamically establish encrypted tunnels between on-premises data centers, branch offices, and cloud regions, offering consistent policies and security controls.

Multi-cloud adoption also drives demand for cloud-native networking functions, such as virtual routers and service meshes, which can be deployed on-demand in cloud environments. These functions integrate with centralized orchestration platforms, enabling enterprises to define intent-based policies that apply across heterogeneous infrastructures. This evolution reflects a broader trend toward software-defined control planes, where routing is no longer tied to physical circuits but to agile overlays that adapt to workload placement and user demand.

The growing reliance on multi-cloud further amplifies the importance of interoperability and open standards. Next-generation routing must support seamless integration across diverse provider ecosystems, requiring collaborative frameworks that promote compatibility. Over time, enterprises will prioritize routing solutions that enable consistent performance, security, and governance across multiple cloud platforms, making next-gen approaches more compelling than legacy MPLS.

Looking to the long-term, MPLS is unlikely to disappear entirely but will instead occupy a specialized role in niche, high-assurance domains. Industries such as finance, defense, and healthcare, which demand deterministic performance, carrier-grade reliability, and strict data sovereignty, will continue to rely on MPLS circuits. For example, financial institutions handling high-frequency trading or defense organizations transmitting classified information may prefer MPLS for its tightly controlled infrastructure and contractual service-level agreements (SLAs).

However, for the vast majority of enterprises, the broad adoption of SD-WAN, segment routing, and intent-based networking is expected to dominate. These technologies provide the agility, scalability, and cost efficiency necessary for organizations operating in distributed, cloud-first environments. By leveraging broadband internet alongside MPLS circuits in hybrid models, enterprises have already demonstrated the value of gradual migration toward next-generation routing. Over time, as internet reliability improves and cloud providers expand their global backbone networks, dependence on MPLS will diminish for most enterprise applications.

Furthermore, the evolution toward segment routing (SR-MPLS and SRv6) represents a bridging point between legacy and next-gen paradigms. Segment routing simplifies traffic engineering by encoding paths directly into packet headers, reducing the complexity of maintaining large label distribution protocols in traditional MPLS. This innovation ensures a smoother migration path for organizations seeking to modernize without discarding their existing MPLS investments.

In the long run, the trajectory points toward adaptive, AI-enhanced, and cloud-native routing ecosystems where MPLS is reserved for specialized, high-assurance workloads and next-gen approaches support the majority of enterprise connectivity needs.

The future of routing technologies will be defined by the integration of AI/ML for predictive optimization, the centrality of multi-cloud strategies, and a dual trajectory where MPLS persists in niche domains while next-generation routing achieves mainstream adoption (Etengu *et al*., 2020; Noack and Sethian, 2021). Enterprises must navigate these shifts by aligning their network strategies with evolving business requirements, regulatory constraints, and technological innovations. By balancing stability and innovation, organizations can build resilient, adaptive, and cost-efficient networks that support the demands of the digital era.

3. Conclusion

The comparative analysis of Multiprotocol Label Switching (MPLS) and next-generation routing frameworks reveals a set of nuanced tradeoffs that enterprises must navigate as they modernize their networking infrastructures. MPLS has long been valued for its deterministic performance, quality of service, and robust service-level agreements, making it a cornerstone of mission-critical applications where latency and reliability are paramount. However, these advantages are accompanied by high operational and capital expenditures, as well as limited flexibility in adapting to the distributed and cloud-centric architectures that now dominate enterprise landscapes. Conversely, next-generation routing paradigms such as SD-WAN, segment routing, and intent-based networking offer agility, cost efficiency, and adaptive performance optimization, yet they often face challenges in achieving carrier-grade reliability when dependent on public internet backbones.

The development of conceptual models that integrate performance, cost, and reliability dimensions provides enterprises with a structured framework for evaluating these tradeoffs. Such models serve as valuable decision-making tools, enabling organizations to map network technologies against their unique operational priorities—whether that entails high-assurance financial transactions, flexible connectivity for remote workforces, or cost-sensitive scaling for startups. By visualizing tradeoff zones, enterprises gain clarity on where MPLS or next-generation solutions, or hybrid combinations of both, align best with their strategic goals.

Looking forward, the networking landscape is converging toward a balance of performance, cost, and reliability, where MPLS retains a role in specialized high-assurance domains while next-generation routing becomes the mainstream enabler of distributed, cloud-integrated enterprises. As AI, automation, and multi-cloud strategies continue to evolve, organizations must adopt adaptive frameworks that reconcile stability with innovation, ensuring that network infrastructures remain resilient, efficient, and future-ready.

4. References

1. Adekunle BI, Chukwuma-Eke EC, Balogun ED, Ogunsola KO. Machine learning for automation: Developing data-driven solutions for process optimization and accuracy improvement. Mach Learn. 2021;2(1).
2. Adeshina YT. Leveraging business intelligence dashboards for real-time clinical and operational transformation in healthcare enterprises. [place unknown: publisher unknown]; [date unknown].
3. Ajayi SAO, Akanji OO. Impact of BMI and menstrual cycle phases on salivary amylase: A physiological and biochemical perspective. [place unknown: publisher unknown]; 2021.
4. Ajayi SAO, Akanji OO. Air quality monitoring in Nigeria's urban areas: Effectiveness and challenges in reducing public health risks. [place unknown: publisher unknown]; 2022.
5. Ajayi SAO, Akanji OO. Efficacy of mobile health apps in blood pressure control in USA. [place unknown: publisher unknown]; 2022.
6. Ajayi SAO, Akanji OO. Substance abuse treatment through telehealth: Public health impacts for Nigeria. [place unknown: publisher unknown]; 2022.
7. Akpan UU, Adekoya KO, Awe ET, Garba N, Oguncoker GD, Ojo SG. Mini-STRs screening of 12 relatives of Hausa origin in northern Nigeria. Niger J Basic Appl Sci. 2017;25(1):48-57.
8. Akpan UU, Awe TE, Idowu D. Types and frequency of fingerprint minutiae in individuals of Igbo and Yoruba ethnic groups of Nigeria. Ruhuna J Sci. 2019;10(1).
9. Alberti AM, Santos MA, Souza R, Da Silva HDL, Carneiro JR, Figueiredo VAC, *et al*. Platforms for smart environments and future internet design: A survey. IEEE Access. 2019;7:165748-78.
10. Alemayehu K. Analyzing impact of segment routing MPLS on QoS. Commun Mag. 2019.
11. Asif R, Ghanem K. AI secured SD-WAN architecture as a latency critical IoT enabler for 5G and beyond communications. In: 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC); 2021 Jan 9-12; [place unknown]. Piscataway (NJ): IEEE; 2021. p. 1-6.
12. Awe ET, Akpan UU. Cytological study of Allium cepa and Allium sativum. [place unknown: publisher unknown]; 2017.
13. Awe ET. Hybridization of snout mouth deformed and normal mouth African catfish Clarias gariepinus. Anim Res Int. 2017;14(3):2804-8.
14. Awe ET, Akpan UU, Adekoya KO. Evaluation of two MiniSTR loci mutation events in five Father-Mother-Child trios of Yoruba origin. Niger J Biotechnol. 2017;33:120-4.
15. Awe T. Cellular localization of iron-handling proteins required for magnetic orientation in C. elegans. [place unknown: publisher unknown]; 2021.
16. Bertoni M. Multi-criteria decision making for sustainability and value assessment in early PSS design. Sustainability. 2019;11(7):1952.
17. Cherukuri BR. Future of cloud computing: Innovations in multi-cloud and hybrid architectures. [place unknown: publisher unknown]; 2019.
18. Chukwuma-Eke EC, Ogunsola OY, Isibor NJ. Designing a robust cost allocation framework for energy corporations using SAP for improved financial performance. Int J Multidiscip Res Growth Eval. 2021;2(1):809-22.
19. Cullen P, Juola C, Karagiannis G, Kivisoo K, Normark M, Rácz A, *et al*. The landscape of hybrid threats: A conceptual model (public version). [place unknown: publisher unknown]; 2021.
20. Ejibenam A, Onibokun T, Oladeji KD, Onayemi HA, Halliday N. The relevance of customer retention to organizational growth. J Front Multidiscip Res. 2021;2(1):113-20.
21. Etengu R, Tan SC, Kwang LC, Abbou FM, Chuah TC. AI-assisted framework for green-routing and load balancing in hybrid software-defined networking: Proposal, challenges and future perspective. IEEE Access. 2020;8:166384-441.
22. Filani OM, Sakyi JK, Okojie JS, Ogedengbe AO. Market research and strategic innovation frameworks for driving growth in competitive and emerging economies. J Front Multidiscip Res. 2022;3(2).
23. Filani OM, Sakyi JK, Okojie JS, Nnabueze SB, Ogedengbe AO. Market research and strategic innovation frameworks for driving growth in competitive and emerging economies. [place unknown: publisher unknown]; 2022.
24. Frangopol DM, Dong Y, Sabatino S. Bridge life-cycle performance and cost: Analysis, prediction, optimisation and decision-making. In: Structures and infrastructure systems. London: Routledge; 2019. p. 66-84.
25. Haensge K, Trossen D, Robitzsch S, Boniface M, Phillips S. Cloud-native 5G service delivery platform. In: 2019 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN); 2019 Nov 12-14; [place unknown]. Piscataway (NJ): IEEE; 2019. p. 1-7.
26. Halliday NN. Assessment of major air pollutants, impact on air quality and health impacts on residents: Case study of cardiovascular diseases [master's thesis]. Cincinnati (OH): University of Cincinnati; 2021.
27. Hummel P, Braun M, Tretter M, Dabrock P. Data sovereignty: A review. Big Data Soc. 2021;8(1):2053951720982012.
28. James T, Olivia B. Optimizing network security and performance with SD-WAN: Next-generation solutions for modern enterprises. Int J Trend Sci Res Dev. 2020;4(4):1891-7.
29. Janssen M, Brous P, Estevez E, Barbosa LS, Janowski T. Data governance: Organizing data for trustworthy Artificial Intelligence. Gov Inf Q. 2020;37(3):101493.
30. John AO, Oyeyemi BB. The role of AI in oil and gas supply chain optimization. Int J Multidiscip Res Growth Eval. 2022;3(1):1075-86.
31. Kansara M. Cloud migration strategies and challenges in highly regulated and data-intensive industries: A technical perspective. Int J Appl Mach Learn Comput Intell. 2021;11(12):78-121.
32. Katsina IA, Johnbull OA, Ovenseri AC. Evaluation of citrus sinensis (orange) peel pectin as a binding agent in Erythromycin tablet formulation. World J Pharm Pharm Sci. 2021;10(10):188-202.
33. Kazim E, Koshiyama A. Explaining decisions made with AI: A review of the co-badged guidance by the ICO and the Turing Institute. SSRN [Internet]. 2020 [cited 2025 Oct 13]. Available from:

https://ssrn.com/abstract=3656269.
34. Knaster R, Leffingwell D. SAFe 5.0 distilled: Achieving business agility with the scaled agile framework. Boston (MA): Addison-Wesley Professional; 2020.
35. Kravchenko M, Pigosso DC, McAloone TC. A trade-off navigation framework as a decision support for conflicting sustainability indicators within circular economy implementation in the manufacturing industry. Sustainability. 2020;13(1):314.
36. Lai V, Chen C, Liao QV, Smith-Renner A, Tan C. Towards a science of human-AI decision making: A survey of empirical studies. arXiv [Internet]. 2021 [cited 2025 Oct 13]. Available from: https://arxiv.org/abs/2112.11471.
37. Leonard AU, Emmanuel OI. Estimation of utilization index and excess lifetime cancer risk in soil samples using gamma ray spectrometry in Ibolo-Oraifite, Anambra State, Nigeria. Am J Environ Sci Eng. 2022;6(1):71-9.
38. Mayr C, Risso C, Grampín E. Crafting optimal and resilient iBGP-IP/MPLS overlays for transit backbone networks. Opt Switch Netw. 2021;42:100635.
39. Mohammad N. Enhancing security and privacy in multi-cloud environments: A comprehensive study on encryption techniques and access control mechanisms. Int J Comput Eng Technol. 2021;12(2):51-63.
40. Mohan TR, Roselyn JP, Uthra RA, Devaraj D, Umachandran K. Intelligent machine learning based total productive maintenance approach for achieving zero downtime in industrial machinery. Comput Ind Eng. 2021;157:107267.
41. Noack MM, Sethian JA. Autonomous discovery in science and engineering. Washington (DC): USDOE Office of Science (SC); 2021.
42. Ogundipe F, Sampson E, Bakare OI, Oketola O, Folorunso A. Digital transformation and its role in advancing the Sustainable Development Goals (SDGs). Transformation. 2019;19:48.
43. Ogunyankinnu T, Onotole EF, Osunkanmibi AA, Adeoye Y, Aipoh G, Egbemhenghe J. Blockchain and AI synergies for effective supply chain management. [place unknown: publisher unknown]; 2022.
44. Ogunyankinnu T, Onotole EF, Osunkanmibi AA, Adeoye Y, Aipoh G, Egbemhenghe JB. AI synergies for effective supply chain management. Int J Multidiscip Res Growth Eval. 2022;3(4):569-80.
45. Oni O, Adeshina YT, Iloeje KF, Olatunji OO. Artificial intelligence model fairness auditor for loan systems. J ID 8993. 2018:1162.
46. Onibokun T, Ejibenam A, Ekeocha PC, Onayemi HA, Halliday N. The use of AI to improve CX in SAAS environment. [place unknown: publisher unknown]; 2022.
47. OnotoleFrancis E, Ogunyankinnu T, Adeoye Y, Osunkanmibi AA, Aipoh G, Egbemhenghe J. The role of generative AI in developing new supply chain strategies—Future trends and innovations. Int J Supply Chain Manag. 2022;11(4):325-38.
48. Onyekachi O, Onyeka IG, Chukwu ES, Emmanuel IO, Uzoamaka NE. Assessment of heavy metals; Lead (Pb), Cadmium (Cd) and Mercury (Hg) concentration in Amaenyi dumpsite Awka. IRE J. 2020;3:41-53.
49. Oyeyemi BB. Artificial intelligence in agricultural supply chains: Lessons from the US for Nigeria. [place unknown: publisher unknown]; 2022.
50. Petricevic O, Teece DJ. The structural reshaping of globalization: Implications for strategic sectors, profiting from innovation, and the multinational enterprise. J Int Bus Stud. 2019;50(9):1487-512.
51. Prasad VK, Bhavsar M. Preserving SLA parameters for trusted IaaS cloud: An intelligent monitoring approach. Recent Pat Eng. 2020;14(4):530-40.
52. Raj P, David GSS. Engineering resilient microservices toward system reliability: The technologies and tools. In: Cloud reliability engineering. Boca Raton (FL): CRC Press; 2021. p. 77-116.
53. Ramdoss Y, Nainar NK. Containers in Cisco IOS-XE, IOS-XR, and NX-OS: Orchestration and operation. Indianapolis (IN): Cisco Press; 2020.
54. Sakyi JK, Filani OM, Nnabueze SB, Okojie JS, Ogedengbe AO. Developing KPI frameworks to enhance accountability and performance across large-scale commercial organizations. J Front Multidiscip Res. 2022;3(2).
55. Sakyi JK, Filani OM, Nnabueze SB, Okojie JS, Ogedengbe AO. Developing KPI frameworks to enhance accountability and performance across large-scale commercial organizations. [place unknown: publisher unknown]; 2022.
56. Shah SDA, Gregory MA, Li S. Cloud-native network slicing using software defined networking based multi-access edge computing: A survey. IEEE Access. 2021;9:10903-24.
57. Shen J, Brower J. Access and edge network architecture and management. In: Future networks, services and management: Underlay and overlay, edge, applications, slicing, cloud, space, AI/ML, and quantum computing. Cham: Springer International Publishing; 2021. p. 157-83.
58. Singi K, Choudhury SG, Kaulgud V, Bose RJC, Podder S, Burden AP. Data sovereignty governance framework. In: Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops; 2020 Jun 27-Jul 19; [place unknown]. New York (NY): ACM; 2020. p. 303-6.
59. Sobhy D, Bahsoon R, Minku L, Kazman R. Evaluation of software architectures under uncertainty: A systematic literature review. ACM Trans Softw Eng Methodol. 2021;30(4):1-50.
60. Thuraka B. AI-driven adaptive route optimization for sustainable urban logistics and supply chain management. Int J Sci Res Comput Sci Eng Inf Technol. 2021;7:667-84.
61. Uriarte RB, De Nicola R, Scoca V, Tiezzi F. Defining and guaranteeing dynamic service levels in clouds. Future Gener Comput Syst. 2019;99:27-40.
62. Vahlne JE, Bhatti WA. Relationship development: A micro-foundation for the internationalization process of the multinational business enterprise. Manag Int Rev. 2019;59(2):203-28.
63. Welsh T, Benkhelifa E. On resilience in cloud computing: A survey of techniques across the cloud domain. ACM Comput Surv. 2020;53(3):1-36.
64. Woods E, Erder M, Pureur P. Continuous architecture in practice: Software architecture in the age of agility and DevOps. Boston (MA): Addison-Wesley Professional; 2021.