International Journal of Leading Research Publication (IJLRP)
E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

Next-Generation Intelligent Multi-Cloud Enterprise Networking: Integrating Secure Architecture, AI-Optimized Traffic Engineering, and LLM-Driven Autonomous Network Operations

Vasantha Kumar Hosahalli Seenappa

Senior Network Engineer/Architect

Abstract:
There has been an increase in the rate of transformation of enterprises digitally and this has resulted in the implementation of multi-cloud environments and allowed organizations to take advantage of the different attributes of Amazon Web Services (AWS), Microsoft Azure and Oracle Cloud Infrastructure (OCI) to develop new, scalable, flexible and resilient ways to services. The growing complexity associated with heterogeneous cloud infrastructures poses multiple challenges with secure inter-cloud connectivity, adequate traffic engineering and autonomous network management. Currently, the majority of approaches to address these challenges do so in a stand-alone manner and produce disjointed security methods, non-optimal traffic optimization and limited operational intelligence. To address these issues, this paper proposes a next-generation intelligent multi-cloud enterprise networking framework that combines secure multi-cloud architecture with AI-optimized traffic engineering and LLM-driven autonomous network operation into one framework. The proposed architecture integrates Zero Trust security principles and AI-based traffic optimization to develop adaptive routing, efficient resource usage and resilient service delivery while using LLMs to automate network configuration, fault finding and remediation of computer systems across distributed cloud environments. By combining these functional components together into one holistic framework, we provide a comprehensive foundation upon which organizations can develop secure, intelligent and self-managing enterprise networks with improved scalability, operational efficiency and adaptability to the future cloud-centric digital infrastructure.

Keywords: Multi-Cloud Enterprise Networking, Cloud Security, Artificial Intelligence (AI), Traffic Engineering, Large Language Models (LLMs), Network Automation, Zero Trust Architecture, Enterprise Cloud Computing.

1. Introduction

Digital transformation is moving quickly and consequently, cloud computing has become the main technology for providing scalable, reliable, and cost-effective computing capabilities throughout all industries and enterprises. Organizations continue to improve their IT infrastructure to allow for data-intensive applications, real-time service delivery, and changing business needs. As enterprise workloads have become more distributed and as operational demands have increased, cloud platforms have transformed from providing basic computing resources into providing adaptable and intelligent digital ecosystems that support complex business functions. This transformation has drastically changed how enterprise networks are designed and maintained, requiring organizations to have more adaptable, resilient, and interconnected cloud infrastructures that are capable of supporting today's computing requirements.

Modern enterprises' strategic imperative to transition from single-cloud deployments to multi-cloud architectures is driven by the increased need for greater scalability, service resiliency, and operational agility. Early research has shown that secure multi-cloud infrastructures are highly successful in supporting mission-critical enterprise workloads and enhancing reliability and ensuring business continuity [1]. The added complexity of distributed cloud computing has resulted in the introduction of advanced cloud security management techniques designed to enhance data protection, access control and threat mitigation for all heterogeneous cloud infrastructures [2]. Complementing this has been the establishment of comprehensive cybersecurity frameworks that emphasize the need to secure hybrid and multi-cloud environments through adaptive security strategies and integrated governance mechanisms [3]. Recent studies have also identified the importance of effective multi-cloud management, resource orchestration and cloud deployment strategies in order to achieve maximum utility of the multi-cloud infrastructure while minimizing the dependency on multiple vendors and the risks associated with operating in such environments [4]-[6]. Currently, most existing capabilities are focused on infrastructure deployment and security management, providing little to no assistance in optimizing traffic intelligently and operating independently within interconnected multi-cloud environments.

The rapid development of enterprise multi-cloud ecosystems has resulted in operational challenges because of the continued expansion in size and complexity. A number of recent publications have discussed the implementation of Zero Trust architectures, AI enabled cloud intelligence platforms, as well as other methods for enhancing authentication, continuous monitoring, and digital trust within decentralized cloud environments [7],[8]. In addition, the use of Artificial Intelligence in multi-cloud infrastructure has shown promise for enhancing resource coordination and efficiency across the network, while hybrid and federated architectures provide additional flexibility for deploying enterprise solutions at scale [9],[10]. Currently existing efforts tend to be focused primarily on single aspects (i.e., security) of enterprise networking instead of integrating securely within a common framework (i.e., security + intelligent traffic engineering + autonomous network management) while successfully achieving interoperability.

Addressing these limitations, an intelligent multi-cloud enterprise networking framework has been proposed that will unite secure multi-cloud architecture, traffic engineering that is optimized for ALE, and autonomous network operations driven by LLM technology, as one complete ecosystem. This framework will reinforce the security of enterprise data with Zero Trust security principles and will optimize inter-cloud traffic with AI-enabled decision-making along with automating all aspects of network configuration, monitoring, fault diagnosis, and troubleshooting with LLM-enabled intelligence. By integrating these capabilities into one cohesive architecture, the framework will ultimately result in better network scalability, operational resiliency, resource efficiency, and productivity of administration. In addition, it will simplify the complexity of managing multi-cloud heterogeneous infrastructures. This framework creates an all-encompassing framework for secure, intelligent self-managing enterprise networks that will support the changing needs of future cloud-driven digital ecosystems.

2. Literature Review

Artificial Intelligence is changing how we manage traffic in very complex Digital Communication networks, known as Traffic Engineering. Historically, most Traffic Engineering was managed using set Routing Rules and Policies, which were static and did not adapt to changing Traffic Patterns and Current Network Conditions. New research has shown that AI-assisted Traffic Engineering Technology will allow Network Operators to continuously carry out Monitoring on their Networks while making Intelligent Decisions regarding Routing of their Data Traffic thus, enhancing Routing Efficiency and Resource Utilization, [11]. Additionally, through Machine Learning and Deep Learning capabilities, Networks can continuously learn from Operational Data and optimize Routing Decisions based on this learned knowledge [13]. With the emergence of Deep Reinforcement Learning (ToADRL), researchers have determined it enables Dynamic Routing and Optimized Traffic Engineering Policies through continuously interacting in Changed Conditions of Complexity within a Network Environment, thus improving Data Latency and Throughput as well as overall Network Performance [14], [15]. All of these advancements make Artificial Intelligence a promising approach to develop Intelligent Enterprise Networks that will enable the growth of Multi-Cloud Infrastructures due to increasing Complexity in Managing Inter-Cloud Communication.

Recent studies on AI-enhanced traffic engineering have also looked at distributing traffic across multi-cloud & SDN environments where intelligent optimization techniques enable dynamic distribution of network traffic across geographically dispersed cloud infrastructures. AI-based traffic optimization has been shown to enhance API communications; balance the traffic load on the network; and improve service reliability in heterogeneous multi-clouds [16]. In addition, the application of deep reinforcement learning to traffic engineering in an SDN environment has allowed for the intelligent selection of routing from multiple routes and the efficient allocation of bandwidth in dynamic network environments [17]. Furthermore, flexible reinforcement learning frameworks are supporting improvements in the area of traffic engineering by adapting router selections based on disturbances in the network whilst maintaining consistent communication performance [18]. Finally, the development of Large Language Models has enabled that the functionality of intelligent network management extends beyond traffic optimization to include automated network configuration, operational assistance and decision support in increasingly complex enterprise networking environments [19].

The development of Large Language Models fully extends the ability to manage intelligent networks autonomously by enabling self-configuration, self-diagnosis of faults, and operational decision support for modern communications networks. Recent studies have highlighted the capability of LLMs to automate the network configuration processes and improve the accuracy of diagnosing faults through context-aware reasoning and intelligent recommendation systems [20], [21]. Additionally, the use of Generative AI, AIOps, and Intent-based Network Management has made it possible to perform predictive maintenance, orchestrate services autonomously, make adaptive decisions, and thus improve next-generation enterprise and enterprise Service Provider (SP) networks' operational efficiency and resilience

[22]-[24]. As such, LLM-powered automation is increasingly driving the development of intelligent and self-managing networks that will support complex cloud computing environments.

Even though many advances have been made on the topic, researchers have mainly focused on secure multi-cloud architectures, traffic engineering using AI, and autonomous network operation with LLM models as three different areas of study, with little to no effort put forth toward designing an enterprise-wide networking framework that combines all these aspects into one cohesive architecture. This has contributed to ongoing issues with securing information across multiple clouds, optimizing traffic in intelligent ways, running networks autonomously, and interoperating between clouds in very complex multi-cloud scenarios. This framework develops and implements an integrated enterprise architecture that combines secure multi-cloud architecture, AI-enabled traffic engineering, and LLM-based autonomous network operation into an all-encompassing intelligent enterprise network environment to improve security, operational efficiency, scalability, and adaptive decision-making. **Table 1** contains a comparative summary of previous studies that relate to this topic area and indicates the research voids that are being closed with the development of the proposed framework.

Table 1. Comparative Summary of Existing Studies on Intelligent Multi-Cloud Enterprise Networking

Author(s) & Year	Methodology / Approach	Domain	Key Contribution	Limitations
Mulder, 2023 [4]	Multi-Cloud Strategy	Enterprise Multi-Cloud Management	Presented enterprise strategies for adopting and managing multi-cloud environments using DevSecOps, FinOps, and BaseOps principles.	Does not incorporate AI-driven traffic engineering or autonomous network management.
Merseedi et al., 2024 [5]	Hybrid & Federated Cloud Architecture Review	Multi-Cloud Computing	Reviewed hybrid and federated cloud architectures for interoperability, scalability, and resource sharing across distributed multi-cloud environments.	Focuses on cloud architecture without intelligent traffic optimization or LLM-based automation.
Kadkhodayi et al., 2023 [11]	AI-Based Real-Time Traffic Management	Intelligent Network Traffic Engineering	Applied Artificial Intelligence for adaptive traffic management and real-time routing decisions.	Limited to traffic optimization without integration into enterprise multi-cloud security frameworks.

Almukhalfi et al., 2024 [13]	Machine Learning & Deep Learning Survey	AI-Based Traffic Engineering	Reviewed ML and DL techniques for intelligent traffic management and routing optimization.	Focuses on AI-based routing without secure multi-cloud orchestration.
Bai et al., 2024 [14]	Deep Reinforcement Learning Routing	Traffic Engineering	Developed an adaptive routing algorithm using Deep Reinforcement Learning for intelligent traffic engineering.	Primarily addresses routing optimization without enterprise cloud security or autonomous management.
Pei et al., 2024 [17]	Deep Reinforcement Learning for SDN	Software-Defined Networking	Proposed an intelligent SDN routing framework for efficient bandwidth allocation and traffic engineering.	Evaluated mainly in SDN environments rather than enterprise multi-cloud infrastructures.
Wang et al., 2024 [19]	LLM-Assisted Network Automation	Intelligent Network Management	Demonstrated how Large Language Models can automate network operation and intelligent decision support.	Focuses mainly on network automation without secure multi-cloud integration.
Wang et al., 2024 [20]	LLM-Based Network Configuration Evaluation	Network Configuration Automation	Evaluated the capability of LLMs for automated network configuration using context-aware reasoning.	Limited emphasis on unified enterprise multi-cloud networking.
Cheng et al., 2023 [22]	AIOps for Cloud Platforms	Enterprise Cloud Operations	Reviewed AI for IT Operations (AIOps) techniques for cloud monitoring, predictive maintenance, and operational automation.	Does not integrate AI traffic engineering and LLM-based autonomous networking into a unified framework.
Mehmood et al., 2023 [23]	Intent-Driven Autonomous Network Management	Autonomous Network & Service Management	Proposed an intent-driven framework for autonomous network and service	Focuses on autonomous service management

			management using policy-driven orchestration.	without secure multi-cloud architecture or AI-based traffic optimization.

The comparison between multiple updated AI-managed networks and multi-cloud orchestration illustrates significant technical issues with developing autonomous decisions across clouds, optimally routing inter-cloud traffic and adaptively configuring networks. These knowledge gaps are the primary drivers for developing an AI-based framework for managing multi-clouds that takes advantage of LLM developed method for gathering intent; optimally engineering inter-cloud routes using intelligent traffic engineering; and monitoring intent with real-time feedback.

3. Proposed Methodology

This proposed methodology incorporates an intelligence-driven framework that uses AI to configure traffic and networks in an autonomous manner, across heterogeneous multi-cloud environments. The framework leverages LLMs, AI-based traffic optimization, automated deployment, continuous monitoring and feedback, and knowledge-based decision making to develop an intelligent and adaptable network management system. The methodology integrates intent-based understanding of terms, policy-based orchestration, real-time telemetry information and continuous feedback to facilitate minimal manual interaction while improving overall network performance, resource utilization, security compliance, and operational efficiency. The methodology consists of multiple functional phases which work together to provide intelligent decision making and closed-loop optimization throughout AWS, Azure, and OCI.

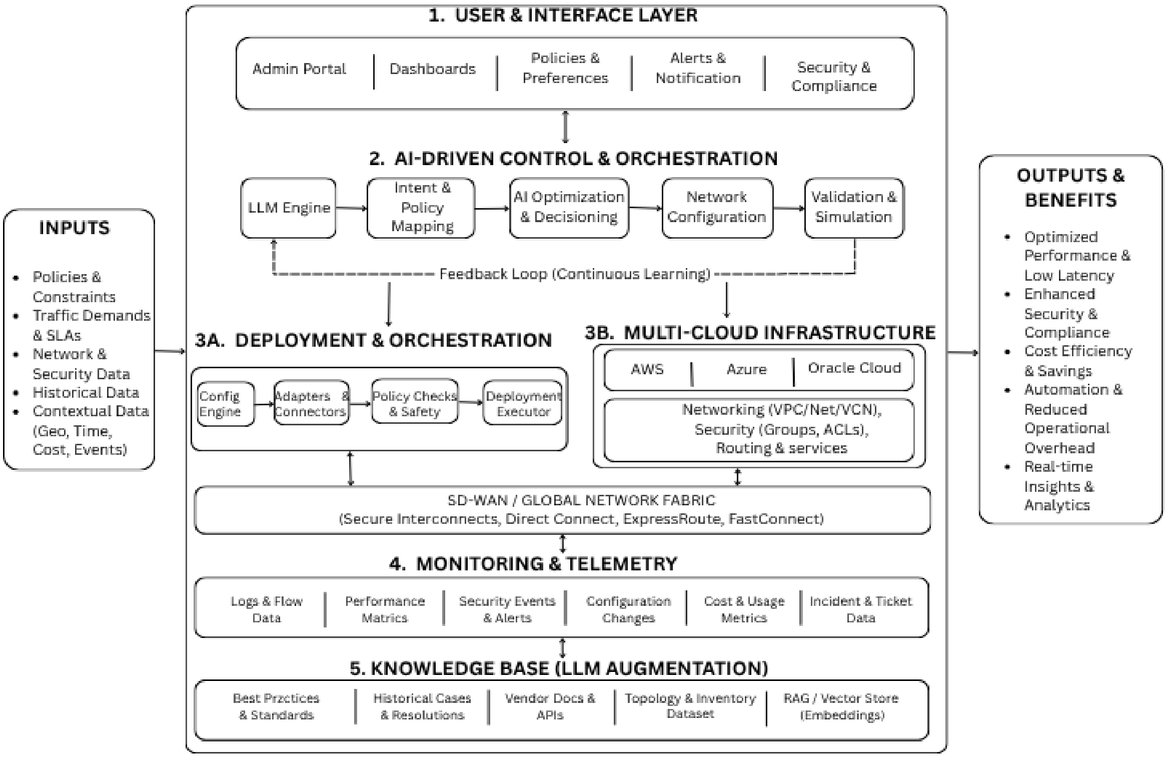

Figure 1. Proposed Architecture

The workflow of our framework is illustrated in Figure 1. In this process, the collected enterprise policies, traffic demands, security needs, and network data are analyzed by a very large language model-based reasoning engine for intent interpretation and policy mapping. Once the decisions are generated, these are optimized, tested, and deployed across Amazon Web Services (AWS), Microsoft Azure (Azure), and Oracle Cloud Infrastructure (OCI). Providing continual feedback to the knowledge base via monitoring and telemetry allows for real-time optimization and intelligent multi-cloud network management.

3.1 Overview of the Proposed Framework

This proposal presents a new unified artificial intelligence architecture that will provide intelligent traffic engineering and autonomous network configuration for heterogeneous multi-cloud environments. The proposed framework will make use of large language models, which will enable high-level network intent to be interpreted and transformed into optimal, policy-compliant network actions through intelligent reasoning and policy mapping. When providing this capability, enterprise policies, service level agreements, security requirements, historical network data, and contextual operational data will be examined to create optimal routing, workload placement, and resource allocation strategies. Equivalent network configurations can automatically be validated and deployed across AWS, Microsoft Azure, and Oracle Cloud Infrastructure (OCI) through cloud native orchestration methods. Additionally, as part of operations, ongoing monitoring and telemetry will provide network performance and security event data as well as configuration change data that will be used to develop a central knowledge base as a basis for adaptive optimization and continuous learning. This integration of autonomous deployment, AI-driven decision making, and closed-loop feedback will create an efficient, scalable, secure, and intelligent multi-cloud network management solution.

3.2 AI-Driven Network Intelligence

The module for AI-Driven Network Intelligence will provide the central decision-making backend of the proposed architecture and as such will facilitate intelligent traffic engineering and policy-aware network optimization within multiple cloud environments. The input to the mechanism is formed from an aggregation of multiple data sets including enterprise policies, service level agreements traffic demands, security requirements, history of network performance and contextually based operational data captured from within a networked environment. The input will be processed through a large language model via intent understanding and policy mapping of high-level administrative objectives into a structured set of network policies.

Interpreted intent with the AI-driven Traffic Engineering module will evaluate current network conditions, and determine optimized routing paths, bandwidth allocations, workload placements, and strategies to utilize resources in line with organizational policies and systems security provisions. The use of LLM-based reasoning combined with intelligent traffic optimization will provide the capability to make adaptive, policy-compliant decisions that will enhance network performance, scalability and operational efficiencies across heterogeneous cloud infrastructures.

3.3 Autonomous Multi-Cloud Deployment

Optimized network policies have been determined using AI-driven decisions, they will be converted into executable configuration files by the Autonomous Multi-Cloud Deployment module. The configuration files generated by the deployment module will go through an automated validation and safety check process so that those configuration files conform to policy compliance, security and deployment consistency before they can be implemented.

The validation process with the deployment engine uses cloud-native APIs and orchestration technologies to automate the provisioning and configuration of network resources across AWS, Microsoft Azure and OCI. Inter-connects and SD-WAN technologies provide seamless communication and traffic flow between various cloud environments enabling reliable connectivity and effective use of cloud resources. This automated deployment approach minimizes the need for human intervention, decreases the incidence of configuration errors, and promotes consistent policy enforcement across heterogeneous multi-cloud infrastructures while supporting scalability, reliability, and operational efficiencies.

3.4 Continuous Monitoring and Knowledge-Based Optimization

Its core, the proposed framework's support for adaptive network management consists of having both a continuous monitoring component and a knowledge-based optimization module that utilizes a closed-loop feedback system. Continuous collection of operational data is done via the deployment of the monitored multi-cloud infrastructure, which includes such things as flow logs, performance metrics, security events, configuration changes, and utilization statistics. This monitored operational data is then stored and organized within a centralized knowledge base that includes all historical cases and vendor documentation and topology information, as well as best practices related to managing and optimizing a multi-cloud environment.

This provides the LLM with the necessary context to refine future reasoning or optimizing decisions. The dynamic capability of the framework will allow for ongoing analysis of telemetry data and iterative incorporation of operational feedback into subsequent decision-making processes so that the framework continuously adjusts to changing network conditions, improves routing efficiency, strengthens security compliance, and enhances the overall reliability and intelligence of managing a multi-cloud network.

4. Performance Analysis and Discussion

Analytical assessment of the proposed AI-based, multi-cloud framework will be conducted based on its architectural design, intelligent decision-making capabilities, and anticipated impact on network management. The proposed framework has an advantage over traditional methods of using static configurations and manual administration by conducting LLM-based reasoning for traffic management, AI-driven traffic engineering, autonomous provisioning, and continuous monitoring in a closed-loop system design.

The real-world deployment has yet occurred to validate the framework; the proposed framework was designed according to well-established networking principles and AI methods documented in the literature. This section provides an overview of the proposed framework's anticipated performance, compares its capabilities to current solutions, explores its potential benefits, outlines its drawbacks, and identifies potential uses in intelligent multi-cloud network management.

4.1 Performance Analysis

AI-driven, multi-cloud framework developed has the potential to improve network performance by implementing LLM-based intent understanding, intelligent traffic engineering, and autonomous network orchestration within a unified closed-loop architecture. This will allow for dynamic analysis of enterprise policies, traffic demands, security needs, and real-time network conditions to provide adaptive routing decisions and optimized resource allocation across different cloud environments. The automatic deployment mechanism will decrease manual configuration time while ensuring policies are consistently enforced and operational efficiency is improved. Continuous monitoring and telemetry will allow the framework to recognize when the network has changed and be able to use operational feedback in later decision-making thanks to a centralized knowledge base.

Comparation with traditional network management methods, this framework offers much higher scalability, creates better security compliance, increases resource utilization, and provides much more automation capability, making it an excellent fit for today's modern multi-cloud enterprises. The benefits of the proposed framework will be evaluated in greater detail through the information in Table 2. It summarizes the functional capabilities associated with each major component as well as provides an overall description of how they interact and contribute to a more intelligent, secure, and effective multi-cloud network management system.

Table 2. Expected Functional Capabilities of the Proposed Framework

Functional Component	Role in the Framework	Expected Outcome
LLM-Based Intent Understanding	Interprets administrator objectives and policies	Accurate policy translation and intelligent decision-making
AI-Driven Traffic Engineering	Optimizes routing and workload distribution	Reduced congestion and improved resource utilization
Autonomous Network Configuration	Generates and validates network configurations	Faster deployment with fewer configuration errors
Multi-Cloud Orchestration	Coordinates AWS, Azure, and OCI resources	Consistent cross-cloud management
Continuous Monitoring & Telemetry	Collects operational and security data	Real-time visibility and adaptive response
Knowledge Base Integration	Stores historical cases and contextual information	Improved reasoning and continuous learning
Closed-Loop Feedback Mechanism	Updates future decisions using telemetry	Adaptive optimization and long-term efficiency

Table 2 also indicates that multiple AI-powered components will be utilized within the overall architecture of the proposed framework to tackle significant obstacles related to multi-cloud networking. The framework consists of three distinct AI-driven technology components which will work together to enhance overall network performance, scalability, and security along with streamlining operations through LLM based reasoning, autonomous orchestration and continuous feedback.

4.2 Discussion

Analytical evaluations, the proposed AI-enhanced multi-cloud framework will be a holistic solution to intelligent network management through the combination of intelligent reasoning using LLM (Long-Lasting Memory), AI-based traffic engineering, autonomous deployment of resources, and real-time continuous monitoring across one seamless architecture. These components together will foster adaptive decision-making, maximize resource usage, and employ policy-aware orchestration and management of heterogeneous cloud environments. In contrast to traditional network management methods that require a lot of manual work, the proposed framework will emphasize automated/continuous optimization and closed feedback loops as a means to achieve effective network control. The proposed framework has not been tested in real-world scenarios; however, it was built upon existing networking principles and recent advances within artificial intelligence and cloud orchestration.

Within the framework, a centralized knowledge base and continuous telemetry were created in order to assist in establishing a more reliable basis for future network decisions and ultimately enhance the scalability, security and operational functionality of the network. Areas for future research may include the practical application of the proposed framework and its effectiveness within the practical implementation of multi-cloud environments, as well as assessing performance against diverse workloads within multiple cloud-based systems in addition to investigating how to apply domain specific LLM's and/or reinforcement learning methods to improve autonomous network management through the proposed framework.

5. Conclusion

This research paper describes a multi-cloud network orchestration framework using AI, intelligent traffic engineering, autonomous network configuration and continuous monitoring of a multi-cloud network to help alleviate the complexities associated with operating in a multi-cloud environment. The integration of intent-based reasoning, policy-aware decision making, automated implementation and knowledge-based optimization into a closed-loop framework is proposed to improve network performance, scalability, security, and operational efficiency while also reducing manual involvement in the orchestration process. The analytical evaluation of this framework shows its ability to adaptively and intelligently manage and orchestrate across AWS, Azure and OCI. While this framework will not be implemented or validated experimentally at this time, the foundation for developing future intelligent networking solutions has been established. As such, future research will include implementing the framework in a real environment, performing experimental performance assessments of the framework, integrating domain-specific LLMs into the framework and evaluating reinforcement learning techniques to improve autonomous decision making and adaptive network optimization.

REFERENCES:

1. Adepu, Rajesh. "Building secure multi-cloud infrastructure for mission-critical enterprise workloads." International Journal of Research Publications in Engineering, Technology and Management (IJRPETM) 5.5 (2022): 14-32.
2. Ajish, D. The Significance of Artificial Intelligence in Zero Trust Technologies: A Comprehensive Review. Journal of Electrical Systems and Information Technology, 2024.
3. Gandhi, N. Zero-Trust Security Models for Multi-Cloud Environments. IJFMR, 2024.
4. Mulder, Jeroen. Multi-Cloud Strategy for Cloud Architects: Learn how to adopt and manage public clouds by leveraging BaseOps, FinOps, and DevSecOps. Packt Publishing Ltd, 2023.

5. Merseedi, K.J., Zeebaree, S.R.M. Cloud Architectures for Distributed Multi-Cloud Computing: A Review of Hybrid and Federated Cloud Environment. Indonesian Journal of Computer Science, 2024.
6. Mulder, J. Multi-Cloud Strategy for Cloud Architects. Packt Publishing, 2023.
7. Singh, H., Sengupta, A., et al. Zero Trust in Multi-Cloud Environments: A Framework for Identity-Aware Micro-Segmentation., 2022.
8. Wang, Danshi, et al. When Large Language Models Meet Optical Networks: Paving the Way for Automation. Electronics, 2024.
9. Kumar, Bharath. "Challenges and solutions for integrating AI with Multi-cloud architectures." International Journal of Multidisciplinary Innovation and Research Methodology, ISSN (2022): 2960-2068.
10. Merseedi, Karwan Jameel, and Subhi RM Zeebaree. "The cloud architectures for distributed multi-cloud computing: a review of hybrid and federated cloud environment." The Indonesian Journal of Computer Science 13.2 (2024).
11. Kadkhodayi, A., et al. "Artificial intelligence-based real-time traffic management." J. Electr. Electron. Eng 2.4 (2023): 368-373.
12. Bai, Jie, et al. An Adaptive Intelligent Routing Algorithm Based on Deep Reinforcement Learning. Computer Communications, 2024.
13. Almukhalfi, Hanan, Ayman Noor, and Talal H. Noor. "Traffic management approaches using machine learning and deep learning techniques: A survey." Engineering Applications of Artificial Intelligence 133 (2024): 108147.
14. Bai, Jie, et al. "An adaptive intelligent routing algorithm based on deep reinforcement learning." Computer Communications 216 (2024): 195-208.
15. Du, Hongyang, et al. "Enhancing deep reinforcement learning: A tutorial on generative diffusion models in network optimization." IEEE Communications Surveys & Tutorials 26.4 (2024): 2611-2646.
16. Henderson, Michael, and Sarah Whitmore. "Intelligent API Traffic Optimization in Multi-Cloud Environments Through Artificial Intelligence."
17. Pei, Xinglong, et al. "Enabling efficient routing for traffic engineering in SDN with Deep Reinforcement Learning." Computer Networks 241 (2024): 110220.
18. Ye, Minghao, et al. "FlexDATE: Flexible and disturbance-aware traffic engineering with reinforcement learning in software-defined networks." IEEE/ACM Transactions on Networking 31.4 (2022): 1433-1448.
19. Wang, Danshi, et al. "When large language models meet optical networks: Paving the way for automation." Electronics 13.13 (2024): 2529.
20. Wang, Changjie, et al. "Netconfeval: Can llms facilitate network configuration?." Proceedings of the ACM on Networking 2.CoNEXT2 (2024): 1-25.
21. Liu, Fan, Farkiani, Behrooz, Crowley, Patrick. A Survey on Large Language Models for Network Operations and Management: Applications, Techniques, and Opportunities., 2024.
22. Cheng, Qian, et al. "Ai for it operations (aiops) on cloud platforms: Reviews, opportunities and challenges." arXiv preprint arXiv:2304.04661 (2023).
23. Mehmood, Kashif, Katina Kralevska, and David Palma. "Intent-driven autonomous network and service management in future cellular networks: A structured literature review." Computer Networks 220 (2023): 109477.
24. Hang, C.N., et al. Large Language Models Meet Next-Generation Networks: A Survey. 2024.
25. Wang, Danshi, et al. When Large Language Models Meet Optical Networks: Paving the Way for Automation. Electronics, 2024.
26. NIST. Zero Trust Architecture (SP 800-207). 2020, or another 2024 enterprise cloud governance paper if you want to keep the topic focused on cloud governance.