International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

Comparative Analysis of Software-Defined Networking and Intent-Based Networking

Sneh Kanwar Singh Sidhu[1], Dr. Sikander Singh Cheema[2]

[1]Email: *snehkanwar26[at]gmail.com*

[2]Email: *sikander[at]pbi.ac.in*

Abstract: ***With the continuous advancement of networking technologies, Software-Defined Networking (SDN) and Intent-Based Networking (IBN) have emerged as prominent paradigms in contemporary network management. SDN offers centralized control of network resources by separating the control plane from the data plane, whereas IBN emphasizes automation by converting high-level business intents into specific network configurations. This research provides a comparative evaluation of SDN and IBN, emphasizing their respective architectures, operational approaches, benefits, limitations, and practical applications. Furthermore, the study explores how both paradigms enhance network agility, security, and efficiency, while examining their potential convergence within future network infrastructures.***

Keywords: Software-Defined Networking (SDN), Intent-Based Networking (IBN), Network Virtualization, Automation, Self-Healing, AI/ML

1. Introduction

Networks have become integral to modern digital infrastructure, facilitating operations across businesses, cloud computing, IoT ecosystems, and large-scale data centers. As network environments grow increasingly complex, conventional management approaches—characterized by static configurations and manual oversight—prove insufficient in meeting evolving demands. The pursuit of greater agility, security, and automation has driven the development of two transformative networking paradigms: Software-Defined Networking (SDN) and Intent-Based Networking (IBN). These approaches redefine network control, management, and optimization. [1] **Software-Defined Networking (SDN)** represents a networking paradigm that decouples the control plane from the data plane, enabling centralized, programmable traffic management. By leveraging software-based controllers, SDN facilitates dynamic traffic handling, policy enforcement, and network programmability, thereby enhancing flexibility. This architectural design improves scalability and simplifies network configuration, making SDN particularly advantageous for cloud computing, data centers, and telecommunication networks. [2] [3] In contrast, **Intent-Based Networking (IBN)** builds on the core principles of SDN but integrates AI-driven automation and high-level policy abstraction. Rather than configuring individual components manually, IBN empowers administrators to define high-level business intents, which the system translates into actionable network configurations. This paradigm leverages machine learning, continuous monitoring, and self-adaptive mechanisms, resulting in a more autonomous and self-optimizing approach to network management. [4] [5] While SDN delivers programmability and centralized control, IBN advances automation through AI-driven decision-making processes. This paper presents a comparative analysis of these paradigms, highlighting their architectures, functionalities, benefits, challenges, and potential intersections in future networking technologies.

2. Software-Defined Networking (SDN)

2.1. Definition and Architecture

Software-Defined Networking (SDN) represents a modernized approach to network architecture, designed to enhance network agility, automation, and management through the separation of the control plane, responsible for traffic routing decisions, from the data plane, which executes packet forwarding according to those decisions. This decoupling enables centralized network management, facilitating the implementation of dynamic policies and efficient traffic optimization. [2] [3] The Software-Defined Networking (SDN) framework is structured into three distinct planes: control, data, and application. At the core, the control plane, managed by the SDN controller, is responsible for overseeing traffic management and implementing policies by maintaining a comprehensive, centralized view of the network. Communication with underlying network devices is facilitated through protocols such as OpenFlow. The data plane, consisting of switches and routers, executes packet forwarding according to the directives issued by the controller. Meanwhile, the application plane enables the development of applications that enhance network capabilities, including security enforcement and traffic optimization. To facilitate interaction, northbound APIs link applications with the controller for real-time monitoring and automation, while southbound APIs establish communication between the controller and network hardware, ensuring efficient command transmission and network control. [6] [7]

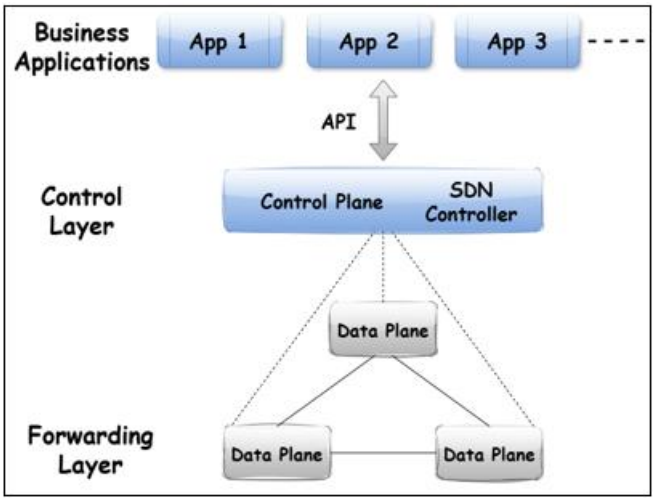

Figure: Software-Defined Networking (SDN)

2.2. Key Features of SDN

SDN introduces several key features that make it more efficient and flexible than traditional networking architectures. Software-Defined Networking (SDN) introduces centralized network control by separating network control functions from forwarding operations, enabling comprehensive and centralized network management. The SDN controller oversees the entire network, allowing for dynamic resource optimization. One of the key advantages of SDN is its programmability and automation. Unlike traditional networks, which require manual and static configurations, SDN facilitates automated and dynamic network configuration. Network behavior can be modified through software-defined policies, eliminating the need for hardware-based adjustments. Additionally, SDN provides dynamic traffic management by enabling fine-grained control over network traffic, adjusting flow routes in real-time. This capability is particularly advantageous in cloud computing and data center environments, where traffic loads frequently fluctuate. In terms of security, SDN enhances network protection through centralized control, which allows for the effective implementation of security policies such as firewalls, access controls, and anomaly detection mechanisms. The centralized approach also enables the dynamic identification and redirection of malicious traffic without manual intervention. Moreover, SDN promotes an open and vendor-neutral network architecture. Unlike traditional networks, which often rely on proprietary solutions from specific vendors, SDN adheres to open standards, reducing dependency on proprietary hardware and fostering interoperability across different platforms. [6-9]

3. Intent-Based Networking (IBN)

3.1. Definition and Architecture

Intent-Based Networking (IBN) is an advanced networking paradigm that builds on the principles of Software-Defined Networking (SDN) but takes automation and intelligence to the next level. IBN introduces a **policy-driven** and **AI-enabled** approach to managing networks, eliminating the need for manual configurations by automatically translating high-level business intents into actionable network policies. IBN shifts the focus from traditional device-centric configurations to intent-driven management. Instead of administrators defining explicit rules and network paths, they specify desired outcomes (intents), such as **"Ensure 99.99% uptime for critical applications"** or **"Prioritize video conferencing traffic over web browsing"**. The IBN system then uses AI, automation, and analytics to configure the network dynamically to achieve these goals. [10] [11] [12]

The Intent-Based Networking (IBN) framework comprises four essential components that transform business objectives into automated network operations. The **Intent Interface (Intent Layer)** facilitates the expression of business goals in a human-readable manner, eliminating the need for complex command-line interface (CLI) configurations. Typical use cases include directives such as "Ensure secure access for remote employees" or "Prioritize bandwidth for VoIP services." The **Translation Engine (Policy Management)** utilizes artificial intelligence (AI) and machine learning (ML) to convert these high-level intents into granular network configurations while maintaining adherence to security policies. The **Automated Deployment and Enforcement (Network Infrastructure)** component employs Software-Defined Networking (SDN) controllers to implement policies across network devices, enabling real-time adjustments without manual intervention. Lastly, **Continuous Monitoring and Assurance** employs AI-driven analytics to track network performance, generating feedback for adaptive self-optimization and fault detection. Collectively, these components drive network automation, performance optimization, and self-healing capabilities within the IBN architecture. [4] [13]

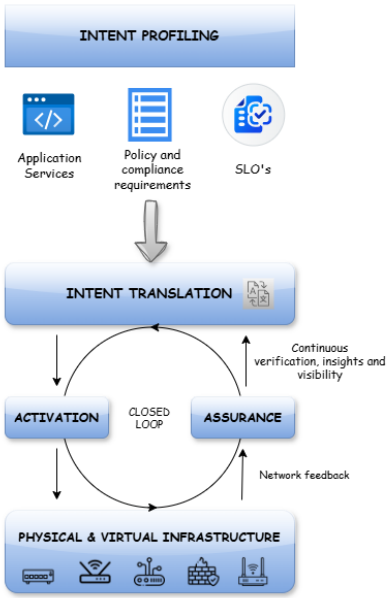

Figure: Intent-Based Networking (IBN)

3.2. Key Features of IBN

Intent-Based Networking (IBN) revolutionizes traditional networking paradigms by incorporating intelligent and automation-driven functionalities. A primary feature of IBN is **AI-driven automation**, which eliminates manual configurations by utilizing artificial intelligence (AI) and machine learning (ML) to enable dynamic network adjustments. Through analysis of historical traffic patterns, IBN autonomously optimizes performance, adapting to

changing conditions without human intervention. IBN also offers **self-adapting and self-healing capabilities**, continuously monitoring network conditions and resolving issues such as traffic rerouting during failures. This proactive approach reduces downtime and minimizes human intervention in network management. A crucial component of IBN is **policy-based control**, where administrators define high-level business objectives, such as prioritizing financial transactions. IBN translates these objectives into network configurations without manual adjustments, streamlining management processes. [17] [18] **Real-time network analytics**, supported by AI-driven insights, detect anomalies, predict failures, and implement preventive measures, enhancing reliability and performance. Additionally, **security automation** enforces predefined security policies, using AI to identify and mitigate threats dynamically, ensuring robust protection. Lastly, **closed-loop assurance** continuously validates compliance with intent-based policies and autonomously corrects performance deviations, maintaining alignment with business objectives and ensuring optimal performance and reliability. [14] [1] [15]

4. Relationship Between SDN and IBN

Intent-Based Networking (IBN) builds upon the core concepts of Software-Defined Networking (SDN), utilizing its programmability and centralized control features to enable advanced automation and intelligent network operations. While SDN emphasizes network programmability, IBN incorporates artificial intelligence (AI)-driven decision-making and self-adaptive capabilities, positioning SDN as a foundational prerequisite. Through AI and machine learning (ML), IBN autonomously analyzes network telemetry, predicts failures, and optimizes performance, ensuring continuous alignment with business policies. A distinguishing feature of IBN is its closed-loop automation, which surpasses SDN's manual adjustments by validating policies in real-time and implementing immediate changes. Additionally, IBN bridges network management and business objectives through high-level intent abstraction, enabling autonomous adjustments aligned with business goals and reducing manual intervention. [21][22].

5. Why SDN Alone is Not Enough

While Software-Defined Networking (SDN) has been pivotal in network programmability, it exhibits certain limitations that Intent-Based Networking (IBN) effectively mitigates through advanced intelligence and automation. One key shortcoming of SDN is its limited context awareness; it primarily manages network states without considering business outcomes or user experience. In contrast, IBN incorporates insights from traffic patterns, latency requirements, and security risks to facilitate more informed decision-making. Additionally, SDN's security mechanisms largely rely on predefined, manually configured rules, whereas IBN employs artificial intelligence (AI) to detect anomalies in real time, enhancing security responsiveness. [23][24].

Scalability is another area where IBN outperforms SDN. The manual configurations required for expanding SDN architectures pose significant challenges in complex networks. IBN addresses this issue through automated policy dissemination across heterogeneous environments, streamlining network expansion. Furthermore, IBN surpasses SDN in maintaining service quality by dynamically adjusting traffic flows and optimizing Quality of Service (QoS) parameters, overcoming the static configuration constraints typical of SDN.

A distinctive advantage of IBN is its self-healing capability, which autonomously identifies and resolves network anomalies, ensuring continuous operation. Additionally, IBN maintains policy compliance through continuous validation mechanisms, eliminating the reliance on manual intervention that characterizes SDN operations. Collectively, these features position IBN as a transformative approach, addressing the inherent limitations of SDN and driving advancements in autonomous network management. [19-21]

How IBN Overcomes SDN Limitations [19-24]

SDN Limitation	How IBN Fixes It
Needs manual updates	Uses AI to auto-adjust configurations dynamically
Lacks proactive security	AI-driven anomaly detection and automated mitigation
Difficult to scale	Automates policy propagation across large networks
Static traffic engineering	Real-time optimization of bandwidth and routing
Manual troubleshooting required	Self-healing capabilities through AI and telemetry
No compliance validation	Continuous policy verification and adaptation

Architectural Comparison

Feature	SDN	IBN
Control Plane	Centralized, software-based SDN controllers manage network traffic.	Higher-level abstraction that translates business intents into policies.
Data Plane	Managed by switches that forward packets based on SDN controller rules.	Similar to SDN, but integrates more automation and optimization.
Intent Processing	Requires manual configuration of network policies.	Translates user-defined intents into automated actions.
Automation Level	High, but still needs human intervention for policy creation.	Fully automated, self-learning, and adaptive.
Monitoring & Telemetry	Uses SDN telemetry for network analytics.	Uses real-time AI-driven telemetry and feedback loops.
Policy Enforcement	Controller enforces rules manually defined by administrators.	Policies are dynamically created and adapted based on AI analysis.

Functional Comparison

Function	SDN	IBN
Network Abstraction	Provides network abstraction via centralized control.	Abstracts intent from low-level configurations.
Flexibility	Enables flexible and programmable networking.	Adds intelligence and adaptability beyond SDN.
Traffic Engineering	Policies are defined manually or through APIs.	AI-driven traffic engineering based on business goals.
Self-Healing	Limited self-healing; requires human intervention.	Automatically detects and resolves network issues.
Security	Uses SDN security policies but still needs manual updates.	Dynamically adapts security measures using AI.

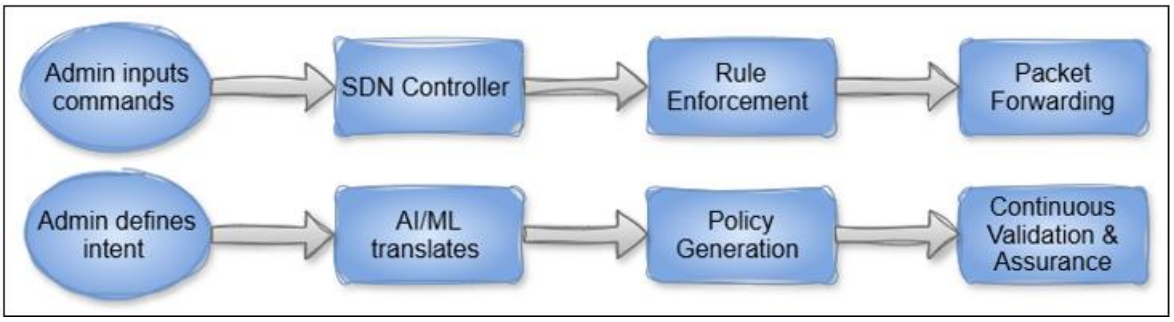

Figure: Intent Processing in IBN vs. SDN Flowchart- visualizing the difference between the two approaches

Use Cases: SDN vs. IBN

Use Case	SDN	IBN
Data Center Networking	Used for managing cloud and virtualized data centers.	Enhances SDN by optimizing workloads and predicting failures.
Service Provider Networks	Enables traffic engineering and slicing.	Automates service provisioning and ensures SLA compliance.
Enterprise Networks	Used for simplifying network management.	Reduces complexity by understanding high-level business intents.
5G & 6G Networks	Supports slicing and software-defined functions.	Enables autonomous, self-optimizing networks.
IoT (Internet of Things)	Provides programmable control for IoT traffic routing.	Adapts to IoT workloads dynamically, ensuring real-time intent-based optimizations.
Cloud Computing & Multi-Cloud Environments	Simplifies cloud network provisioning via SDN controllers.	Automates cloud workload balancing, optimizes performance, and predicts failures.
Network Security & Threat Mitigation	Implements SDN-based security policies manually.	Uses AI-driven security automation to detect and respond to threats proactively.
Edge Computing	Supports edge traffic management and connectivity.	Dynamically provisions network resources for optimal performance at the edge.
Autonomous Vehicles & V2X Communication	Implements network slicing for connected vehicles.	Ensures ultra-reliable low-latency communication (URLLC) with AI-driven optimizations.
Telemedicine & Smart Healthcare	Supports programmable healthcare networks.	Guarantees QoS for remote surgery and telemedicine using intent-based prioritization.
Industrial Automation (Industry 4.0)	Manages software-defined networks in factories.	Ensures predictive maintenance and adaptive network configurations for industrial IoT (IIoT).
Blockchain-Based Networks	Uses SDN for optimizing blockchain transaction routing.	Automates blockchain security policies and optimizes network resources based on demand.

[12] [14] [16] [25-32]

Challenges & Limitations: SDN vs. IBN

Challenge	SDN	IBN
Complexity	Requires knowledge of SDN controllers, APIs, and OpenFlow programming.	AI models need extensive training, requiring specialized expertise in AI and networking.
Deployment Cost	Lower than IBN but still requires SDN controllers, network reconfiguration, and skilled engineers.	High due to AI/ML integration, intent translation engines, and real-time data analytics tools.
Interoperability	Works well with OpenFlow, NETCONF, and API-based systems but requires vendor support for full integration.	Needs AI-driven orchestration to support multi-vendor and multi-domain environments.
Scalability	Can scale but requires manual intervention to optimize large-scale networks.	Highly scalable due to automation, but computational costs for AI-driven decisions increase with network size.
Security & Trust	Centralized control plane is a potential security risk if the SDN controller is compromised.	AI-based decisions may introduce vulnerabilities if the intent translation process is flawed or manipulated.
Policy Enforcement	Policies must be manually defined and programmed, requiring periodic updates.	Policies are dynamically enforced but need reliable intent interpretation and feedback mechanisms.
Troubleshooting & Debugging	Debugging issues require human intervention and deep knowledge of SDN controllers.	AI-driven decision-making can be a "black box," making it harder to trace issues and validate corrective actions.
Network Resilience	Can recover from failures but requires manual reconfiguration of backup paths.	Self-healing capabilities enable automatic anomaly detection and recovery, but AI models must be well-trained.

Adaptability to Dynamic Environments	Reacts to network changes based on predefined policies but lacks real-time adaptability.	Continuously learns and adapts using AI but depends on high-quality telemetry and intent accuracy.
Data Dependency	Relies on static configurations and periodic monitoring data.	Requires real-time telemetry, large datasets, and accurate AI models for continuous optimization.
Regulatory & Compliance Issues	Compliance depends on manual configurations and security policies.	AI-driven automation may struggle to comply with strict regulatory frameworks and audit requirements.
AI & ML Reliability	Lacks AI-driven decision-making; network changes rely on human-defined rules.	AI/ML algorithms require training, validation, and continuous updates to avoid incorrect network behaviors.
Vendor Lock-In	Many SDN solutions are proprietary, limiting interoperability.	IBN solutions depend on AI models and vendor-specific intent processing, which can lead to stronger vendor lock-in.

6. Future Directions

A promising avenue for future research in Intent-Based Networking (IBN) involves conducting comprehensive reviews that trace its evolution from Software-Defined Networking (SDN). Potential directions include performing a systematic literature review to address challenges in intent translation, evaluating existing solutions, and identifying their limitations. Additionally, a comparative analysis of AI and ML applications in IBN for autonomous decision-making could provide insights into their efficacy. Investigating IBN's integration with emerging technologies such as 5G, 6G, and cloud computing may uncover prevailing trends and research gaps. [34][4]. Furthermore, a survey examining security concerns in both IBN and SDN, with a focus on intent verification and policy enforcement, could contribute valuable perspectives on risk mitigation. Finally, an analysis of standardization and interoperability initiatives may offer a clearer understanding of progress toward achieving unified architectural frameworks in IBN. [1][15].

7. Conclusion

This research presents a comparative analysis of Software-Defined Networking (SDN) and Intent-Based Networking (IBN), emphasizing their distinctions in architecture and operational mechanisms. SDN offers centralized control and programmable network management, though it relies heavily on manual configurations. Building upon SDN principles, IBN integrates AI-driven intent processing, automation, and closed-loop feedback mechanisms, fostering enhanced network autonomy and adaptability. The study highlights IBN's advantages in intelligent decision-making, self-healing capabilities, and policy-based management, while also addressing challenges such as increased system complexity, issues with interpretability, and implementation overhead. To advance IBN frameworks, future research should prioritize improvements in security mechanisms and intent translation techniques, contributing to the evolution of self-governing, user-centric networking solutions.

References

[1] Gharbaoui, M., Martini, B., & Castoldi, P. (2023, July). Intent-Based Networking: Current Advances, Open Challenges, and Future Directions. In *2023 23rd International Conference on Transparent Optical Networks (ICTON)* (pp. 1-5). IEEE.

[2] Kim, H., & Feamster, N. (2013). Improving network management with software defined networking. *IEEE Communications Magazine*, *51*(2), 114-119.

[3] Nunes, B. A. A., Mendonca, M., Nguyen, X. N., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Communications surveys & tutorials*, *16*(3), 1617-1634.

[4] Pang, L., Yang, C., Chen, D., Song, Y., & Guizani, M. (2020). A survey on intent-driven networks. *IEEE Access*, *8*, 22862-22873.

[5] Yu, H., Rahimi, H., Janz, C., Wang, D., Li, Z., Yang, C., & Zhao, Y. (2024). Building a Comprehensive Intent-Based Networking Framework: A Practical Approach from Design Concepts to Implementation. *Journal of Network and Systems Management*, *32*(3), 1-22.

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

[7] Xia, W., Wen, Y., Foh, C. H., Niyato, D., & Xie, H. (2014). A survey on software-defined networking. *IEEE Communications Surveys & Tutorials*, *17*(1), 27-51.

[8] Masoudi, R., & Ghaffari, A. (2016). Software defined networks: A survey. *Journal of Network and computer Applications*, *67*, 1-25.

[9] Benzekki, K., El Fergougui, A., & Elbelrhiti Elalaoui, A. (2016). Software-defined networking (SDN): a survey. *Security and communication networks*, *9*(18), 5803-5833.

[10] Szilágyi, P. (2021). I 2 BN: Intelligent Intent Based Networks. *Journal of ICT Standardization*, *9*(2), 159-200.

[11] A Clemm, L Ciavaglia, LZ Granville, J Tantsura "Intent-Based Networking - Concepts and Defnitions", RFC 9315 IETF 2022. [Online]. Available: https://datatracker.ietf.org/doc/rfc9315/

[12] "Intent-Based Networking and Extending the Enterprise White Paper", Cisco White paper. Online. Available: https://www.cisco.com/c/en/us/solutions/collateral/internet-of-things/nb-09-intent-based-iot-wp-cte-en.html

[13] Mehmood, K., Kralevska, K., & Palma, D. (2023). Intent-driven autonomous network and service management in future cellular networks: A structured literature review. *Computer Networks*, *220*, 109477.

[14] Saha, B. K., Tandur, D., Haab, L., & Podleski, L. (2018, October). Intent-based networks: An industrial perspective. In *Proceedings of the 1st international workshop on future industrial communication networks* (pp. 35-40).

[15] Mahdi, M. F., & Mahmoud, M. S. (2022). A Structured Literature Review of Intent Based Network for Future Networks. *Journal of Optoelectronics Laser*, *41*(4), 677-684.

[16] Szigeti, T., Barton, R., Henry, J., & Zacks, D. (2021). INTENT-BASED NETWORKING FROM THE IOT EDGE TO THE APPLICATION SERVER.
[17] DAVOLI, G. INTENT-BASED APPROACH TO VIRTUALIZED INFRASTRUCTURE MANAGEMENT IN SDN/NFV DEPLOYMENTS.
[18] Beshley, M., Veselý, P., Pryslupskyi, A., Beshley, H., Kyryk, M., Romanchuk, V., & Kahalo, I. (2020). Customer-oriented quality of service management method for the future intent-based networking. *Applied sciences*, *10*(22), 8223.
[19] Hyder, M. F., Fatima, T., & Arshad, S. (2024). Digital forensics framework for intent-based networking over software-defined networks. *Telecommunication Systems*, *85*(1), 11-27.
[20] Singh, A., Aujla, G. S., & Bali, R. S. (2020). Intent-based network for data dissemination in software-defined vehicular edge computing. *IEEE Transactions on Intelligent Transportation Systems*, *22*(8), 5310-5318.
[21] Han, Y., Li, J., Hoang, D., Yoo, J. H., & Hong, J. W. K. (2016, October). An intent-based network virtualization platform for SDN. In *2016 12th International Conference on Network and Service Management (CNSM)* (pp. 353-358). IEEE.
[22] Martini, B., Gharbaoui, M., & Castoldi, P. (2022). Intent-based zero-touch service chaining layer for software-defined edge cloud networks. *Computer Networks*, *212*, 109034.
[23] Davoli, G., Cerroni, W., Tomovic, S., Buratti, C., Contoli, C., & Callegati, F. (2019). Intent-based service management for heterogeneous software-defined infrastructure domains. *International Journal of Network Management*, *29*(1), e2051.
[24] Song, Y., Feng, T., Yang, C., Mi, X., Jiang, S., & Guizani, M. (2023). IS2N: Intent-driven security software-defined network with blockchain. *IEEE Network*, *38*(3), 118-127.
[25] Rafiq, A., Afaq, M., & Song, W. C. (2020). Intent-based networking with proactive load distribution in data center using IBN manager and Smart Path manager. *Journal of Ambient Intelligence and Humanized Computing*, *11*(11), 4855-4872.
[26] Njah, Y., Leivadeas, A., Violos, J., & Falkner, M. (2023). Toward intent-based network automation for smart environments: A healthcare 4.0 use case. *IEEE Access*, *11*, 136565-136576.
[27] Abbas, K., Khan, T. A., Afaq, M., & Song, W. C. (2021). Network slice lifecycle management for 5g mobile networks: An intent-based networking approach. *IEEE Access*, *9*, 80128-80146.
[28] Cerroni, W., Buratti, C., Cerboni, S., Davoli, G., Contoli, C., Foresta, F., ... & Verdone, R. (2017, July). Intent-based management and orchestration of heterogeneous openflow/IoT SDN domains. In *2017 IEEE Conference on Network Softwarization (NetSoft)* (pp. 1-9). IEEE.
[29] Martini, B., Gharbaoui, M., & Castoldi, P. (2023). Intent-based network slicing for SDN vertical services with assurance: Context, design and preliminary experiments. *Future Generation Computer Systems*, *142*, 101-116.
[30] Zhang, J., Yang, C., Dong, R., Wang, Y., Anpalagan, A., Ni, Q., & Guizani, M. (2023). Intent-driven closed-loop control and management framework for 6G open RAN. *IEEE Internet of Things Journal*.
[31] **"**Solving Data Centre Pain Points With Intent-Based Networking", A PACKET PUSHERS WHITEPAPER, 2020. Online. Available: https://www.juniper.net/content/dam/www/assets/white-papers/us/en/2021/packet-pushers-solving-data-center-pain-points-with-intent-based-networking.pdf
[32] Huang, J., Yang, C., Kou, S., & Song, Y. (2022, October). A brief survey and implementation on ai for intent-driven network. In *2022 27th Asia pacific conference on communications (APCC)* (pp. 413-418). IEEE.
[33] Jeff Doyle, "Intent-Based Networking for dummies", Online. Available: https://www.juniper.net/content/dam/www/assets/ebooks/us/en/intent-based-networking-for-dummies.pdf
[34] Wei, Y., Peng, M., & Liu, Y. (2020). Intent-based networks for 6G: Insights and challenges. *Digital Communications and Networks*, *6*(3), 270-280.