AUIQ Technical Engineering Science

Manuscript 1045

Recent Trends in Network Technologies: A Comprehensive Review

Atheer Y. Oudah

Raaid Alubady

Lina M. Shaker

AUIQ TECHNICAL ENGINEERING SCIENCE 2025;2:61–96

REVIEW

Recent Trends in Network Technologies: A Comprehensive Review

Atheer Y. Oudah [a], Raaid Alubady [a], Lina M. Shaker [b,*]

[a] Al-Ayen Scientific Research Center, Al-Ayen Iraqi University, AUIQ, An Nasiriyah, P.O. Box: 64004, Thi Qar, Iraq
[b] Laser and Optoelectronics Engineering Department, College of Engineering, Al-Ayen Iraqi University, Nile St, Nasiriyah, Dhi Qar, 64001, Iraq

ABSTRACT

The networking domain is undergoing profound transformation, driven by the rapid maturation of artificial intelligence, edge computing, and advanced virtualization technologies. This review analyzes the major networking trends that have emerged between 2010 and 2025, emphasizing their technological foundations, practical implementation challenges, and long-term implications for the evolution of digital infrastructure. Specifically, it analyzes advances in network function virtualization, AI-enabled network operations, edge computing integration, and the evolution of next-generation connectivity standards. This review highlights the interplay and convergence of these technologies, arguing that their combined adoption is not merely incremental but represents a paradigm shift in network design, deployment, and management. The findings suggest that such convergence has the potential to significantly enhance performance, minimize latency, and strengthen reliability, while addressing the escalating demands of modern digital infrastructure. By emphasizing these intersecting dynamics, the review contributes a forward-looking perspective on the unique opportunities and challenges that will define the next phase of networking innovation.

Keywords: Network, AIOps, Edge computing, 400 gigabit ethernet, Zero trust

1. Introduction

Modern networking infrastructure faces unprecedented demands from data-intensive applications, IoT proliferation, and the need for real-time processing capabilities. The digital transformation accelerated by global events has fundamentally altered how organizations approach network design, deployment, and management. Traditional networking models, which relied heavily on static configurations and hardware-based solutions, are giving way to dynamic, software-defined architectures that can adapt to changing business requirements in real-time [1, 2]. The convergence of artificial intelligence, edge computing, and advanced networking protocols is creating new paradigms that promise to enhance performance, reduce latency, and improve network reliability. These technologies are not developing in isolation but are interconnected, with each advancement enabling and amplifying the capabilities of others. For instance, AI-powered network operations require robust edge computing infrastructure to process data locally, while edge computing deployments depend on high-speed, low-latency networking to maintain connectivity with centralized resources [3, 4]. The scope of this transformation extends beyond technical capabilities to encompass fundamental changes in how organizations approach network architecture, security, and operations. The shift toward cloud-native applications, the proliferation of IoT devices, and the increasing demand for real-time analytics are driving requirements that traditional networking approaches cannot adequately address [5, 6]. The networking industry is experiencing a period of

Received 6 July 2025; revised 2 September 2025; accepted 2 September 2025.
Available online 16 September 2025

* Corresponding author.
E-mail addresses: atheer@alayen.edu.iq (A. Y. Oudah), alubadyraaid@alayen.edu.iq (R. Alubady), linamohmmed91@gmail.com (L. M. Shaker).

https://doi.org/10.70645/3078-3437.1045

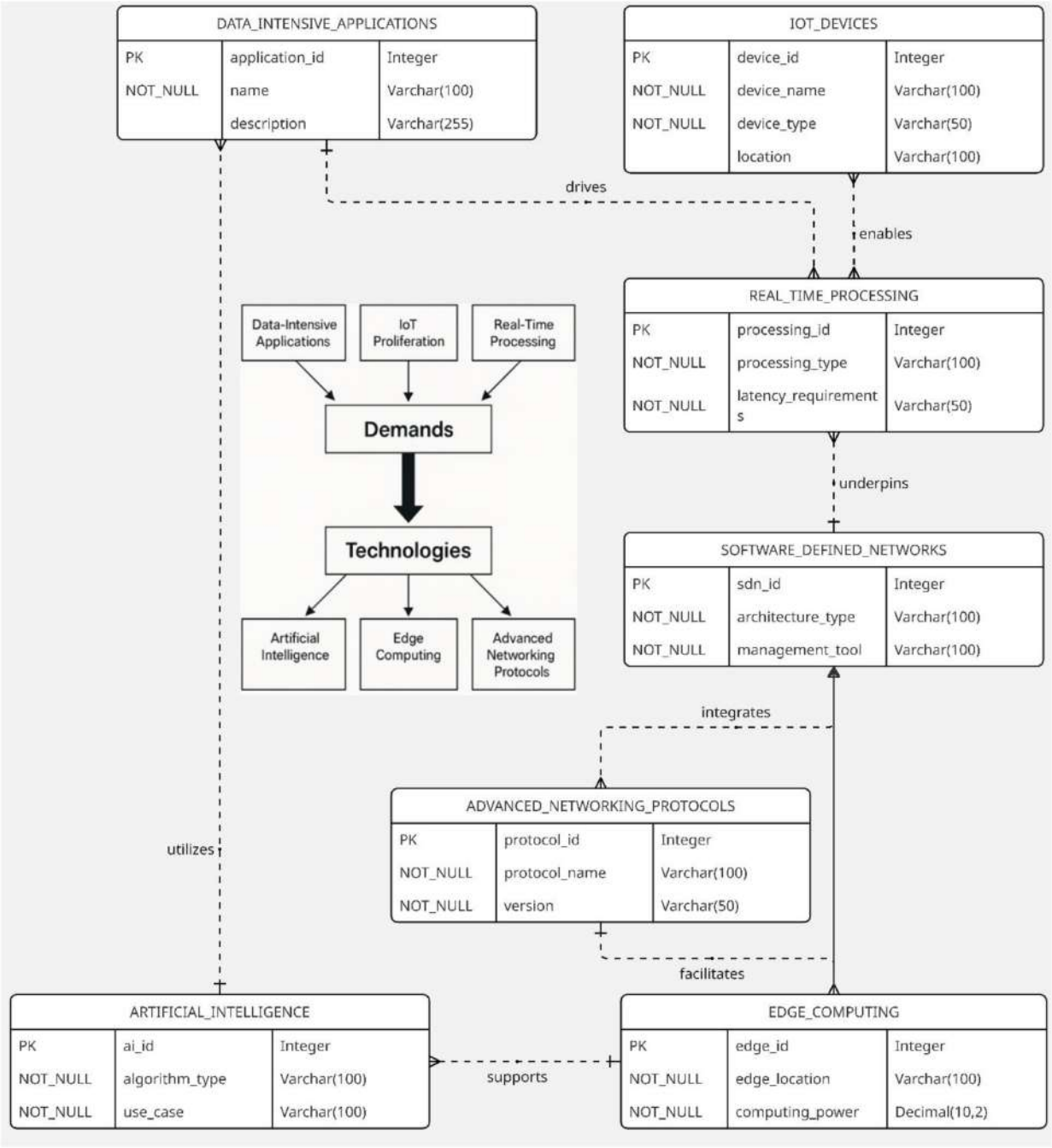

Fig. 1. Modern networking infrastructure.

unprecedented innovation, with new technologies and approaches emerging at a rapid pace. Organizations must navigate this complex landscape while balancing the need for innovation with the requirements for stability, security, and cost-effectiveness. The decisions made today regarding network architecture and technology adoption will have long-lasting implications for organizational capabilities and competitive positioning [7, 8]. Fig. 1 illustrating the key drivers and enabling technologies of modern networking infrastructure. Data-intensive applications, IoT proliferation, and real-time processing demands fuel the adoption of technologies like artificial intelligence, edge computing, and advanced networking protocols working in a tightly interconnected ecosystem to support dynamic, software-defined network architectures. This comprehensive review examines the most significant networking trends of 2010-2025,

analyzing their technological foundations, implementation challenges, and potential impact on future network design. We explore how these trends are interconnected and how organizations can leverage them to build more capable, efficient, and resilient network infrastructure.

2. Network function virtualization and software-defined networking

2.1. Market evolution and technological foundations

Network Function Virtualization (NFV) is a transformative networking paradigm that decouples network functions such as firewalls, proxies, load balancers, and intrusion detection systems from proprietary hardware appliances, enabling them to run as software on commodity hardware platforms. This approach eliminates the dependency on dedicated hardware, making network services more flexible, scalable, and cost-efficient. In practice, these functions are instantiated as NFVs, which can be dynamically chained to form a Service Function Chain (SFC) that delivers the requested service flow end to end [9]. The global NFV market has experienced robust growth, driven by the shift from hardware-based to software-based infrastructures. By leveraging virtualization, organizations can provision and scale services on demand, accelerating time-to-market and reducing capital expenditures. This shift also complements Software-Defined Networking (SDN), which provides centralized programmability and orchestration of network resources, allowing VNFs to be deployed and managed with greater agility [10].

The technological foundation of NFV rests on several key principles that distinguish it from traditional networking approaches. First, the decoupling of network functions from proprietary hardware enables organizations to implement network services using standard servers, storage, and switches [11]. This decoupling provides unprecedented flexibility in how network services are deployed, scaled, and managed. Second, the virtualization of network functions allows for dynamic resource allocation, enabling organizations to scale services up or down based on demand without requiring physical hardware changes. The architectural benefits of NFV extend beyond simple cost reduction to encompass fundamental improvements in operational efficiency and service agility [12]. VNFs can be instantiated, configured, and terminated programmatically, enabling organizations to implement network services on-demand [13]. This capability is particularly valuable in cloud environments where workloads can scale rapidly and unpredictably. Additionally, NFV enables the implementation of service chaining, where multiple network functions can be linked together to create complex service topologies that would be difficult or impossible to implement using traditional hardware-based approaches [14]. The integration of NFV with SDN creates synergistic benefits that enhance the capabilities of both technologies. SDN provides the centralized control plane that can orchestrate NFVs, while NFV provides the virtualized data plane services that SDN can direct and manage. This integration enables organizations to implement highly flexible, programmable network architectures that can adapt to changing requirements in real-time [15, 16]. The technological foundations of NFV are depicted in Fig. 2, which organizes the transition from hardware appliances to virtualized services into a clear operational sequence. As shown, NFV first enables virtualized services, which are then deployed to run on standard servers. These servers provide the necessary hardware specifications and operating systems to host network functions. The next stage illustrates how virtualized services utilize network functions, which are abstracted into software-based modules with defined configurations. Finally, the model demonstrates how these network functions are delivered as service outcomes, defined by delivery method and quality of service. This ordered progression highlights the architectural shift from tightly coupled, vendor-specific appliances to modular, software-defined services. By explicitly decoupling network functions from hardware and sequencing their interactions, NFV enables programmable orchestration, scalability, and adaptability to modern digital infrastructure demands.

2.2. Implementation strategies and best practices

The successful implementation of NFV requires careful planning and consideration of multiple factors including performance requirements, integration complexity, and operational procedures. Organizations must develop comprehensive implementation strategies that address both technical and operational aspects of NFV deployment. The migration from traditional hardware-based network functions to virtualized alternatives typically follows a phased approach, starting with less critical functions and gradually expanding to more mission-critical services [17, 18]. Performance optimization represents one of the most critical challenges in NFV implementation. NFVs must deliver performance levels comparable to or exceeding those of traditional hardware-based solutions. This requires careful attention to resource allocation, including CPU, memory, and network

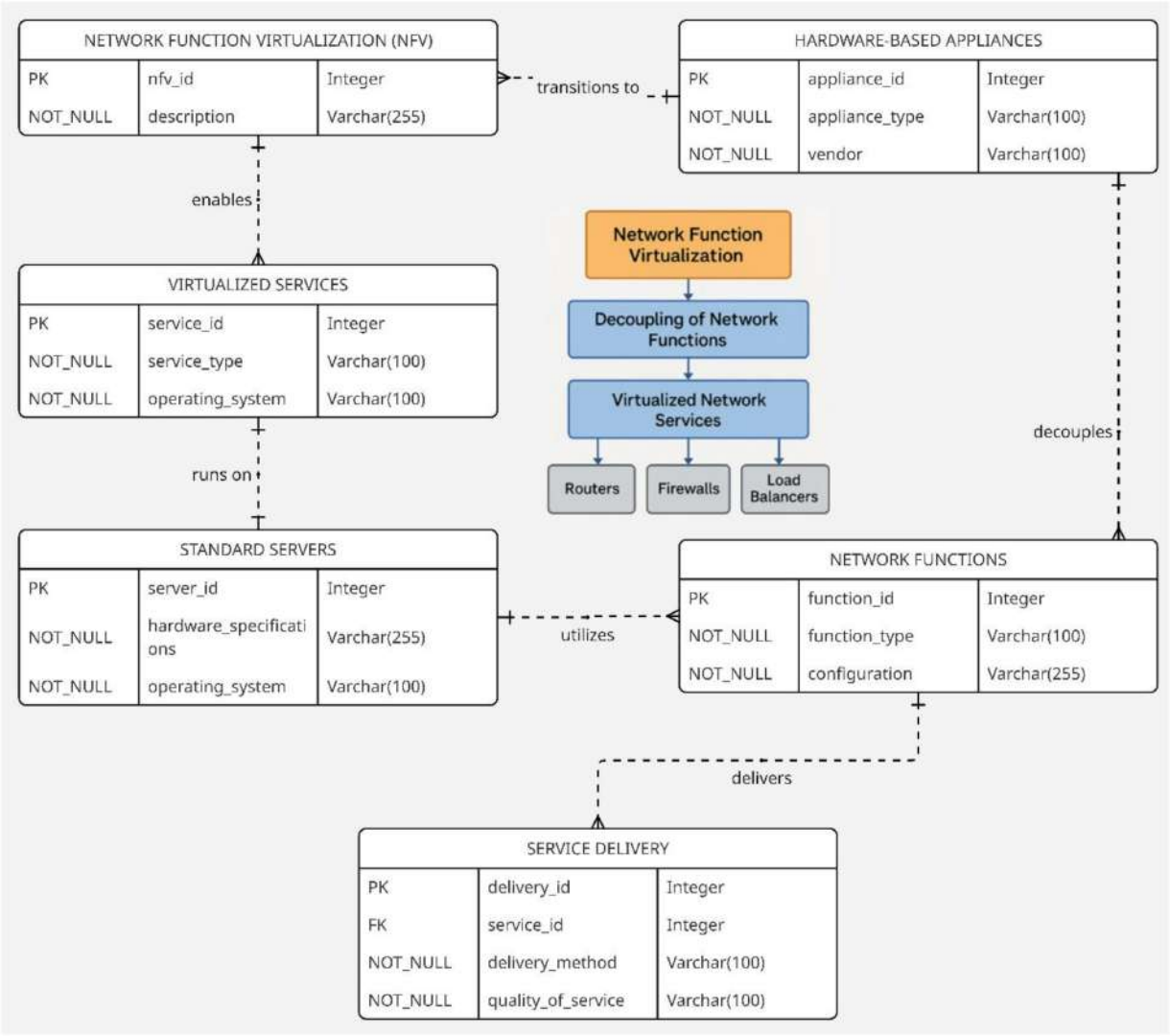

Fig. 2. The transition from hardware-based appliances (e.g., routers, firewalls, load balancers) to software-driven virtualized services that run on standard servers.

bandwidth. Organizations must implement performance monitoring and optimization procedures to ensure that NFVs meet service level requirements. Additionally, the placement of NFVs on appropriate hardware platforms is crucial for achieving optimal performance [19, 20]. The integration of NFV with existing network infrastructure requires careful consideration of compatibility and interoperability issues. Organizations must ensure that NFVs can integrate seamlessly with existing network management systems, security policies, and operational procedures. This often requires the development of custom integration solutions and the modification of existing operational processes. The complexity of this integration should not be underestimated, as it can significantly impact the timeline and cost of NFV deployment [21, 22]. Operational transformation is another critical aspect of NFV implementation. The shift from hardware-based to software-based network functions requires new skills and operational procedures. Network operations teams must develop expertise in virtualization technologies, software deployment and management, and automated orchestration systems. This transformation often requires significant investment in training and may necessitate changes in organizational structure and processes [23, 24]. Fig. 3 outlining the core components for successful NFV deployment. It highlights phased migration, performance optimization, infrastructure integration, and operational transformation as key pillars each supported by best practices such as gradual transition, system compatibility, skills development, and training investment to ensure seamless and effective implementation.

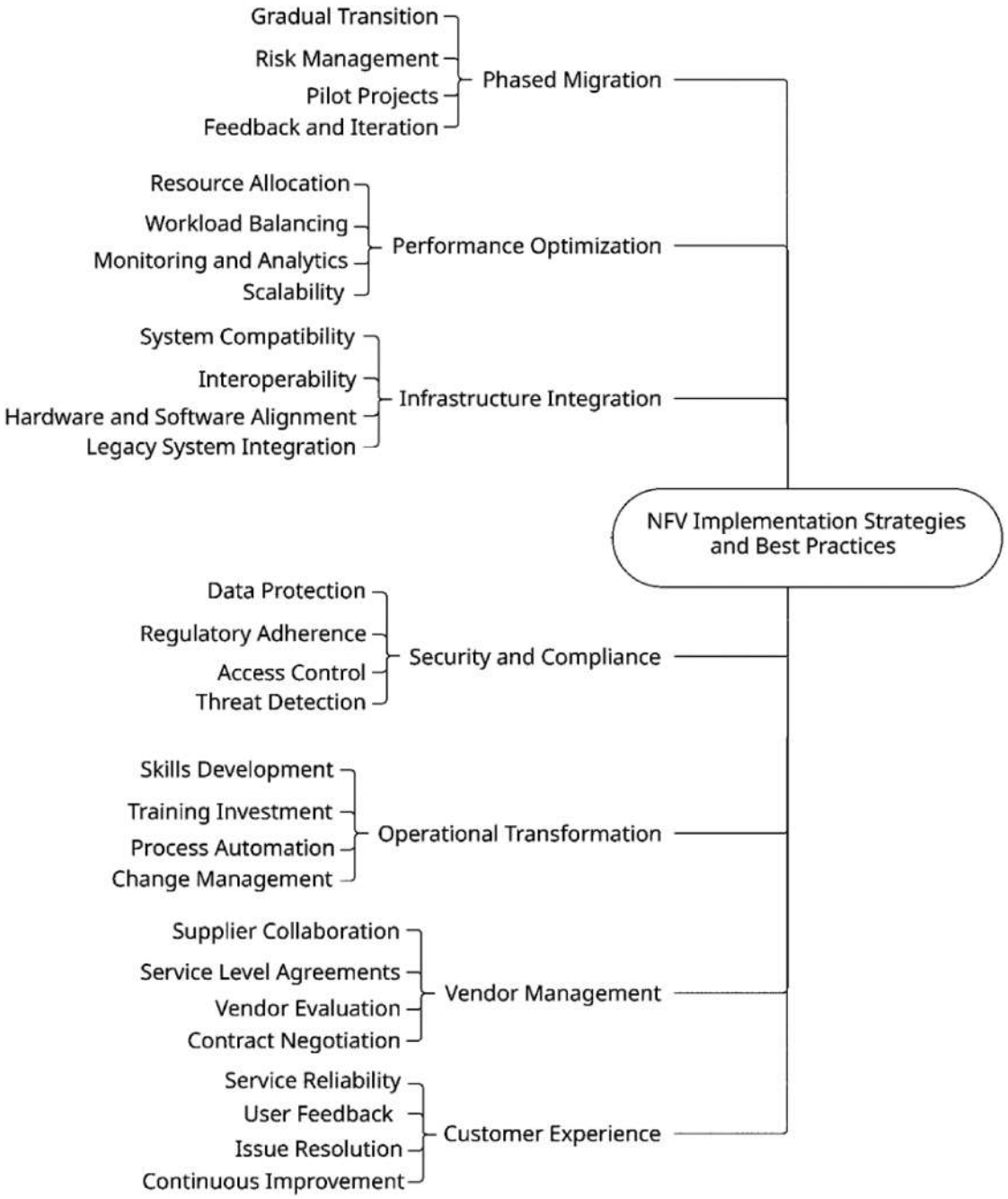

Fig. 3. NFV Implementation Strategies and Best Practices.

2.3. Challenges and future directions

Despite the significant benefits of NFV, organizations face several challenges in implementation and operation. Performance optimization remains a primary concern, as NFVs must deliver consistent performance under varying load conditions. The overhead associated with virtualization can impact performance, particularly for functions that require high packet processing rates or low latency. Organizations must implement sophisticated performance monitoring and optimization strategies to address these challenges [25, 26]. Security considerations in NFV environments are complex and multifaceted. NFVs introduce new attack vectors and security challenges that must be addressed through comprehensive security frameworks. The dynamic nature of virtualized environments requires security policies that can adapt to changing configurations and deployments. Additionally, the shared infrastructure used by

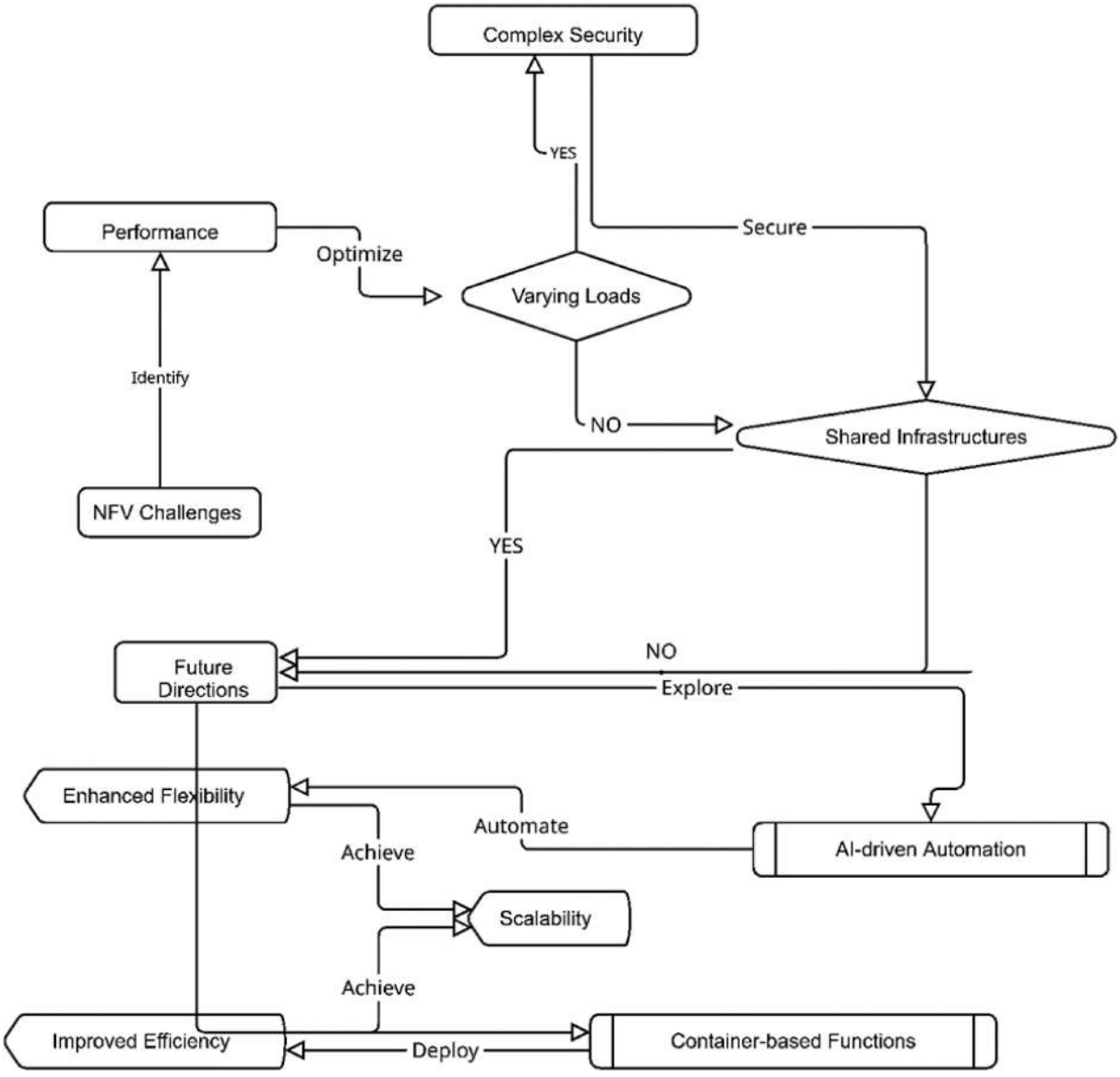

Fig. 4. Challenges and Future Directions of NFV according to the literature.

NFVs can introduce security risks that do not exist in traditional hardware-based deployments [27, 28]. The standardization of NFV technologies and interfaces remains an ongoing challenge. While industry organizations have developed standards for NFV architectures and interfaces, the implementation of these standards varies among vendors and platforms. This lack of standardization can complicate multi-vendor deployments and limit the portability of NFVs across different platforms [29, 30]. Looking toward the future, NFV technology is expected to continue evolving to address current limitations and enable new capabilities. The integration of artificial intelligence (AI) and machine learning (ML) technologies into NFV platforms promises to enhance automation and optimization capabilities. Additionally, the development of container-based network functions offers the potential for improved performance and resource efficiency compared to traditional virtual machine-based approaches [31, 32]. Fig. 4 illustrating the key challenges and emerging future directions in NFV. Challenges include performance optimization under varying loads and complex security considerations in shared infrastructures. Future directions emphasize AI-driven automation and container-based network functions as promising advancements for enhancing flexibility, efficiency, and scalability in NFV deployments.

3. AI-powered network operations (AIOps)

3.1. Intelligent network management revolution

AI is revolutionizing network operations through automated monitoring, predictive analytics, and intelligent troubleshooting capabilities. AIOps platforms represent a fundamental shift from reactive network management to proactive, intelligent systems that can analyze vast amounts of network data in real-time, identifying patterns and anomalies that would be impossible for human operators to detect manually. This transformation is driven by the increasing complexity of modern network environments and the need for more efficient, reliable network operations [33, 34]. The technological foundation of AIOps rests on several key AI and ML technologies. ML algorithms enable systems to learn from historical network data and identify patterns that indicate potential issues or optimization opportunities. Natural language processing capabilities allow AIOps platforms to analyze unstructured data sources such as network logs, trouble tickets, and documentation to extract relevant information for decision-making. Deep learning techniques enable the analysis of complex, multi-dimensional network data to identify subtle patterns and correlations that traditional monitoring tools might miss [35, 36]. The implementation of AIOps requires sophisticated data collection and analysis capabilities. Modern networks generate enormous volumes of data from various sources including network devices, applications, security systems, and user interactions. AIOps platforms must be capable of ingesting, processing, and analyzing this data in real-time to provide actionable insights. This requires robust data integration capabilities, scalable processing infrastructure, and sophisticated analytical algorithms [36, 37]. The benefits of AIOps extend beyond simple automation to encompass fundamental improvements in network reliability, performance, and efficiency. Intelligent monitoring systems can detect potential issues before they impact users, enabling proactive remediation that prevents service disruptions. Predictive analytics capabilities allow organizations to anticipate capacity requirements, optimize resource allocation, and plan infrastructure upgrades more effectively [38, 39]. Additionally, AIOps can significantly reduce the time required to diagnose and resolve network issues, improving overall operational efficiency. Fig. 5 illustrating the core components of AIOps in intelligent network management. The diagram highlights how automated monitoring, predictive analytics, data collection and analysis, and intelligent troubleshooting converge to enable real-time, AI-driven network operations that enhance performance, reliability, and operational efficiency in complex digital environments.

3.2. Predictive performance optimization

AI-enabled networks can predict peak loads and adjust network pathways before bottlenecks occur, representing a fundamental shift from reactive to proactive network management [41]. This predictive capability is essential for maintaining consistent service levels across complex, dynamic network environments [42]. The implementation of predictive performance optimization requires sophisticated modeling techniques that can analyze historical performance data, identify patterns and trends, and make accurate predictions about future network behavior.

The technological foundation of predictive optimization integrates several components. Time series analysis techniques reveal patterns in network performance data, including seasonal variations and trend changes. ML algorithms, particularly ensemble methods and deep learning architectures, provide superior accuracy compared to traditional statistical approaches. For instance, Farooq et al. (2021) demonstrated that ensemble learners such as random forests and adaptive boosting outperform individual models in predicting complex outcomes, achieving high Coefficient of Determination (R^2) values with reduced errors in high-performance concrete modeling [42]. Similarly, Huo et al. (2021) applied random forest feature selection combined with convolutional neural networks to predict proton-exchange membrane fuel cell behavior, showing that deep learning models with dropout and batch normalization can reduce overfitting while improving generalization [43]. Zhang et al. (2021) reported that gradient boosting regression (GBR) and random forest (RF) models effectively predicted and optimized bio-oil production, with GBR yielding test R^2 values above 0.85 [44]. Guo et al. (2023) further advanced predictive modeling by coupling physical mechanism models with long short-term memory (LSTM) neural networks for runoff forecasting, where optimal model combinations reduced RMSE by over 60% and improved R^2 by more than 24% during validation [45]. These findings demonstrate that predictive optimization benefits from combining diverse modeling strategies. As summarized in Table 1, ensemble learners have shown high predictive accuracy in handling non-linear traffic patterns, convolutional neural networks (CNNs) are effective for capturing spatial-temporal dependencies in traffic flows, and LSTM networks excel at sequential prediction of usage peaks. In networking

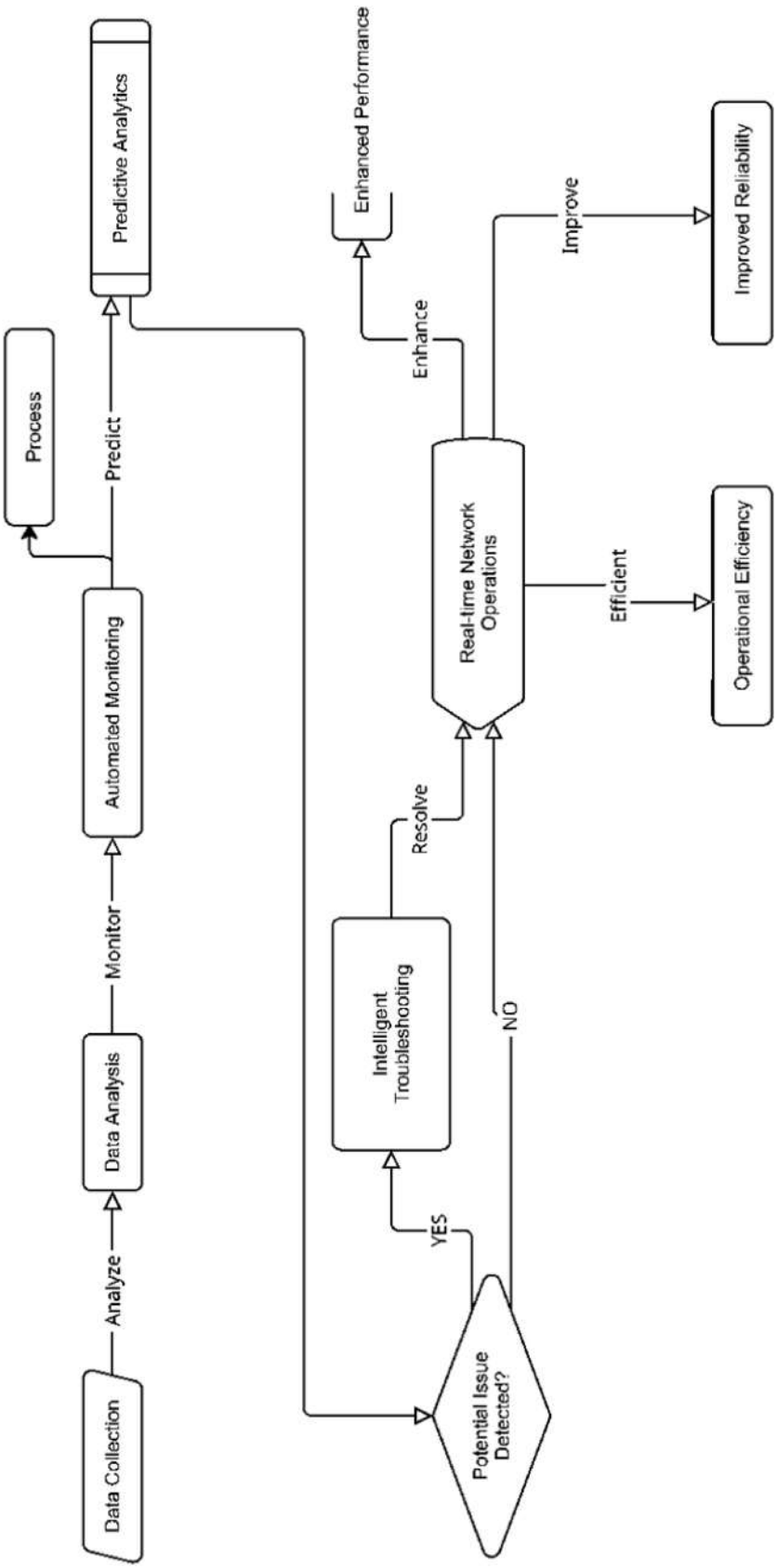

Fig. 5. AIOps workflow, where the data is collected and analyzed through automated monitoring, enabling predictive analytics to forecast potential issues. Detected anomalies are addressed using intelligent troubleshooting, feeding back into real-time network operations.

Table 1. ML techniques for predictive network performance optimization.

ML Technique	Application in Network Optimization	Reported Performance
Random Forest (Farooq et al., 2021; Zhang et al., 2021)	Resource usage prediction, anomaly detection, feature selection	Achieved R^2 up to 0.92 in complex prediction tasks; robust for high-dimensional data with reduced errors.
Gradient Boosting Regression (Zhang et al., 2021)	Performance optimization under multiple parameters	Test R^2 consistently >0.85; outperformed RF in multi-target predictions for optimization tasks.
Convolutional Neural Networks (Huo et al., 2021)	Spatial-temporal traffic analysis, feature extraction	Delivered highly accurate predictions of fuel cell I–V curves; dropout and batch normalization improved generalization.
LSTM Neural Networks (Guo et al., 2023)	Traffic time-series forecasting, sequential load prediction	Reduced RMSE by $>60\%$ and increased R^2 by 24% in validation; effective for long-term dependency modeling.
Ensemble Learners (Bagging/Boosting, Farooq et al., 2021)	Predicting peak loads, improving resilience of models	Enhanced predictive accuracy compared to individual learners; strong performance stability across varied datasets.

contexts, applying these techniques alongside real-time data processing from routers, switches, firewalls, and applications is essential to ensure continuous optimization and consistent service quality.

3.3. Automated incident response and resolution

ML algorithms are being deployed to automate incident detection and response, representing a significant advancement in network operations efficiency. These systems can learn from historical incidents to improve their response accuracy over time, creating a continuous improvement cycle that enhances network reliability and reduces operational costs. The implementation of automated incident response requires sophisticated analytical capabilities, comprehensive knowledge bases, and robust automation frameworks [46, 47]. The technological foundation of automated incident response includes several key components. Pattern recognition algorithms enable the identification of incident signatures and symptoms, allowing systems to detect potential issues before they escalate. Natural language processing capabilities allow systems to analyze unstructured data sources such as logs, alerts, and documentation to extract relevant information for incident analysis. Building on this, Manda (2024) highlights how AI-powered threat intelligence platforms in the telecom sector leverage advanced ML algorithms to perform real-time anomaly detection and intelligence gathering, enabling proactive measures against potential breaches before they escalate [48]. Similarly, Akhtar and Rawol (2024) demonstrate that AI-driven cybersecurity systems, incorporating machine learning, natural language processing, and anomaly detection, can identify subtle patterns indicative of cyberattacks, while also addressing the challenges of adversarial AI and the need for transparent, interpretable models to strengthen trust in automated systems [49].

The implementation of automated incident response thus requires attention to classification, escalation, and safeguards. Kumar et al. (2025) show that AI-driven tools for network monitoring significantly enhance incident response and resilience by combining continuous traffic analysis, intrusion prevention, and predictive analytics, thereby reducing the risk of undetected threats [50]. Furthermore, Farzaan et al. (2024) propose an AI-enabled incident response framework for cloud environments that integrates network traffic classification, web intrusion detection, and malware analysis, emphasizing the importance of intelligent escalation and human oversight in managing complex or critical incidents [51].

The benefits of automated incident response extend beyond simple cost reduction to encompass significant improvements in network reliability and user satisfaction. Automated systems can respond to incidents much faster than human operators, reducing the time to resolution and minimizing service impact. Additionally, automated systems can consistently apply best practices and procedures, reducing the risk of human error and improving the quality of incident response. The ability to learn from historical incidents enables continuous improvement in response accuracy and effectiveness. Table 2 represents a comparative analysis of manual versus AI-driven automated incident response in modern network operations.

4. Edge computing integration

4.1. Edge-to-cloud continuum architecture

The integration of edge computing with traditional cloud infrastructure is creating hybrid models that balance centralized and decentralized processing capabilities. This approach represents a fundamental shift in how organizations architect their

Table 2. Comparison between manual and automated incident response.

Criteria	Manual Response	Automated Response
Response Time	Minutes to hours	Seconds to minutes
Scalability	Limited	High
Accuracy	Variable	Consistent (improves with learning)
Human Error Risk	High	Low
Knowledge Utilization	Depends on individual	Centralized knowledge base
Learning from History	Ad hoc	Continuous ML-based improvement

Table 3. Edge vs. cloud vs. hybrid deployment comparison.

Attribute	Edge Computing	Cloud Computing	Hybrid (Edge-to-Cloud)
Latency	Ultra-low	Moderate to High	Tuned to application needs
Data Processing Location	On-device/local gateway	Centralized data centers	Distributed (edge + cloud)
Use Case Examples	AR/VR, autonomous vehicles, industrial IoT	Analytics, AI training, cloud apps	Smart cities, real-time analytics, 5G services
Security Surface Area	High (many distributed points)	Moderate	High but controllable with orchestration
Bandwidth Usage	Low (local processing)	High (raw data sent to cloud)	Optimized through filtering and caching

computing infrastructure, moving from purely centralized cloud models to distributed architectures that can process data and execute applications closer to their source. The edge-to-cloud continuum enables organizations to optimize performance, reduce latency, and improve efficiency by placing computing resources where they are most needed [52]. The architectural foundation of edge computing integration rests on several key principles that distinguish it from traditional cloud-centric approaches. First, the distribution of computing resources across multiple tiers enables organizations to process data at the optimal location based on factors such as latency requirements, bandwidth constraints, and privacy considerations. Second, the seamless integration between edge and cloud resources allows applications to leverage the benefits of both local processing and centralized resources as needed. Third, the dynamic orchestration of workloads across edge and cloud resources enables organizations to adapt to changing requirements and conditions in real-time [53, 54]. The implementation of edge computing integration requires sophisticated orchestration and management capabilities. Organizations must be able to deploy, configure, and manage applications and services across multiple edge locations and cloud environments. This requires robust orchestration platforms that can handle the complexity of distributed deployments while maintaining consistency and reliability. Additionally, the management of edge resources requires new operational procedures and tools that can handle the unique challenges of distributed infrastructure [55, 56]. The networking implications of edge computing integration are significant and multifaceted. Edge deployments require robust, low-latency connectivity to both end users and centralized cloud resources. This often necessitates the implementation of new networking technologies and architectures, including software-defined WAN (SD-WAN) solutions, edge-optimized protocols, and advanced quality of service (QoS) mechanisms [57]. Additionally, the security implications of distributed edge deployments necessitate advanced orchestration and policy-enforcement mechanisms, as highlighted by Ullah et al. (2021), who demonstrate through MiCADO-Edge that managing applications across the cloud-to-edge continuum requires continuous monitoring, runtime management, and context-aware access control to ensure both performance and data protection in sensitive domains such as healthcare [58]. Table 3 summarizes comparison of deployment characteristics, latency performance, and application relevance across edge, cloud, and hybrid computing models.

4.2. Real-time processing and ultra-low latency applications

Edge computing is becoming essential for applications requiring ultra-low latency, such as autonomous vehicles, industrial automation, and augmented reality experiences. These applications generate massive amounts of data that must be processed immediately to ensure safety and performance. The traditional approach of sending all data to centralized cloud resources for processing introduces latency that is unacceptable for these critical applications. Edge computing enables local processing that can meet the stringent latency requirements of these applications while maintaining connection to centralized resources for less time-sensitive operations [59, 60]. The technological requirements for real-time

Table 4. Latency requirements and division of processing responsibilities across edge and cloud environments for representative applications.

Application	Latency Requirement	Edge Processing Role	Cloud Involvement
Autonomous Vehicles	<10 ms	Object detection, sensor fusion, decision-making	Navigation map updates
Industrial Robotics	<20 ms	Real-time control loop, failover logic	Historical analysis and reporting
Augmented Reality (AR)	<30 ms	Spatial tracking, frame rendering	Asset updates and backups
Remote Surgery	<5 ms	Real-time actuator control and haptics	Record keeping and imaging storage

processing at the edge are demanding and require careful consideration of multiple factors. Processing capabilities at edge locations must be sufficient to handle the computational requirements of real-time applications while maintaining consistent performance under varying load conditions. Storage capabilities must provide fast access to frequently used data while maintaining synchronization with centralized data stores. Networking capabilities must provide reliable, low-latency connectivity to both end users and centralized resources [61, 62]. The implementation of real-time processing at the edge requires sophisticated application architectures that can effectively distribute processing across edge and cloud resources. Applications must be designed to handle the complexity of distributed processing while maintaining consistency and reliability. This often requires the implementation of new programming models and frameworks that can handle the unique challenges of edge computing environments. Additionally, the deployment and management of real-time applications at the edge requires new operational procedures and tools [63, 64]. The benefits of real-time processing at the edge are significant and enable new categories of applications and services. By processing data locally, organizations can achieve latency levels that are impossible with centralized cloud processing. This enables applications such as autonomous vehicles, industrial automation, and augmented reality that require immediate response to local conditions [65]. Additionally, local processing can reduce bandwidth requirements and improve overall system efficiency by processing data where it is generated rather than transmitting it to centralized locations. Table 4 is a latency thresholds and division of labor between edge and cloud in real-time applications, emphasizing where edge computing is indispensable. The table highlights how different domains exhibit strict latency thresholds ranging from less than 5 ms in remote surgery to under 30 ms in augmented reality that necessitate edge computing for real-time processing tasks such as sensor fusion, actuator control, and spatial tracking. Meanwhile, the cloud assumes complementary roles focused on non-latency-critical operations such as navigation map updates, historical data analysis, and long-term storage. This division of responsibilities underscores the critical role of edge processing in meeting ultra-low latency requirements, while the cloud provides scalability, persistence, and large-scale analytical support.

4.3. IoT device management and scalability

With billions of IoT devices expected to be online, edge computing provides the necessary infrastructure to manage and process data from these devices efficiently. The scale of IoT deployments presents unprecedented challenges for traditional networking and computing architectures as shown in Fig. 6. Aruna and Pradeep (2020) show that container technologies can significantly improve scalability in IoT and Fog of Things environments by supporting multitasking, clustering, and distributed service management, thereby enhancing network efficiency and computation control [66]. Similarly, Bellavista, Corradi, and Zanni (2017) highlight that integrating mobile IoT with cloud and fog computing offers scalable solutions by effectively combining local edge resources with globally distributed cloud infrastructures [67].

The architectural requirements for IoT device management at the edge are therefore complex and multifaceted. Bali et al. (2020) propose a rule-based auto-scalability mechanism for IoT services that uses lightweight containers and orchestration to enable adaptive resource utilization across heterogeneous clusters, ensuring responsiveness in dynamic environments [68]. Complementing this, Mavromatis et al. (2019) introduce a software-defined IoT management framework (SDIM) that leverages SDN-enabled edge architectures, demonstrating experimentally that it reduces provisioning times by up to 46% and fault detection times by 33% compared to conventional approaches [69].

The networking implications of large-scale IoT deployments are also profound. Babar and Khan (2021) emphasize that scalable frameworks must address latency and energy efficiency through techniques like recursive clustering and prioritized task offloading, which extend device lifetime while maintaining quality of service [70]. Expanding this perspective, Kuchuk and Malokhvii (2024) review the integration of IoT with cloud, fog, and edge paradigms, conclud-

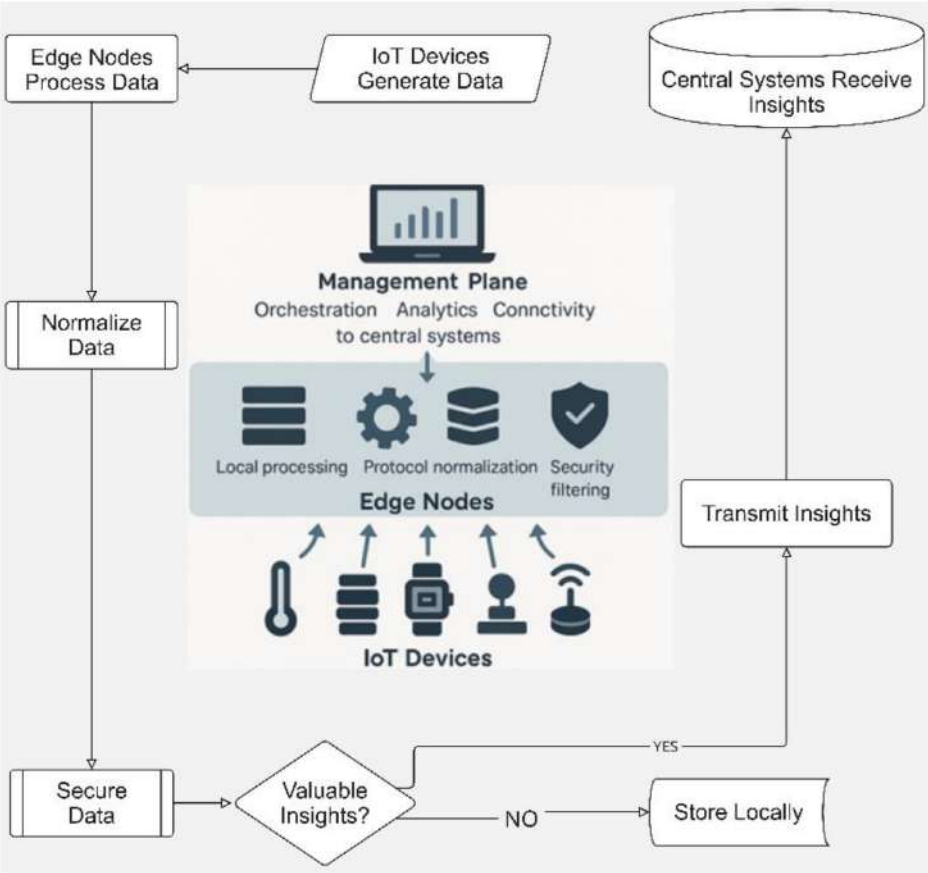

Fig. 6. Data flow and management processes in large-scale IoT deployments using edge computing.

ing that hybrid frameworks are essential for achieving real-time processing, bandwidth efficiency, and robust security in large-scale IoT ecosystems [71].

Finally, the implementation of IoT device management at the edge requires sophisticated data processing and analytics capabilities. Hong and Varghese (2019) survey architectures and algorithms for fog/edge resource management, underscoring the difficulty of managing heterogeneous and resource-constrained devices at scale [72]. Likewise, Ren et al. (2018) argue that edge computing enables real-time and context-aware services by distributing computation closer to devices, but stress that future research must tackle challenges in distributed data management, collaboration with cloud services, and privacy protection [73].

5. High-speed ethernet and next-generation connectivity

5.1. 400 Gigabit ethernet deployment and market dynamics

The deployment of 400 Gigabit Ethernet (400GbE) switches has accelerated significantly, with substantial year-over-year growth in datacenter deployments. This high-speed connectivity represents a crucial evolution in networking infrastructure, enabling organizations to support increasingly bandwidth-intensive applications and maintain performance in modern data centers. The transition to 400GbE is driven by several factors including the growth of cloud computing, the proliferation of high-definition video content, and the increasing computational requirements of AI and ML applications [74, 75]. The technological foundation of 400GbE represents a significant advancement over previous Ethernet standards. The achievement of 400 Gbps throughput requires sophisticated signal processing techniques, advanced error correction mechanisms, and high-performance optical transceivers. The implementation of 400GbE also requires careful consideration of power consumption, heat generation, and physical space requirements. Modern 400GbE switches incorporate advanced cooling systems and power management capabilities to address these challenges while maintaining reliable operation [76, 77]. The market dynamics driving 400GbE adoption are complex and multifaceted. The increasing demand for bandwidth-intensive applications such as 4K and 8K

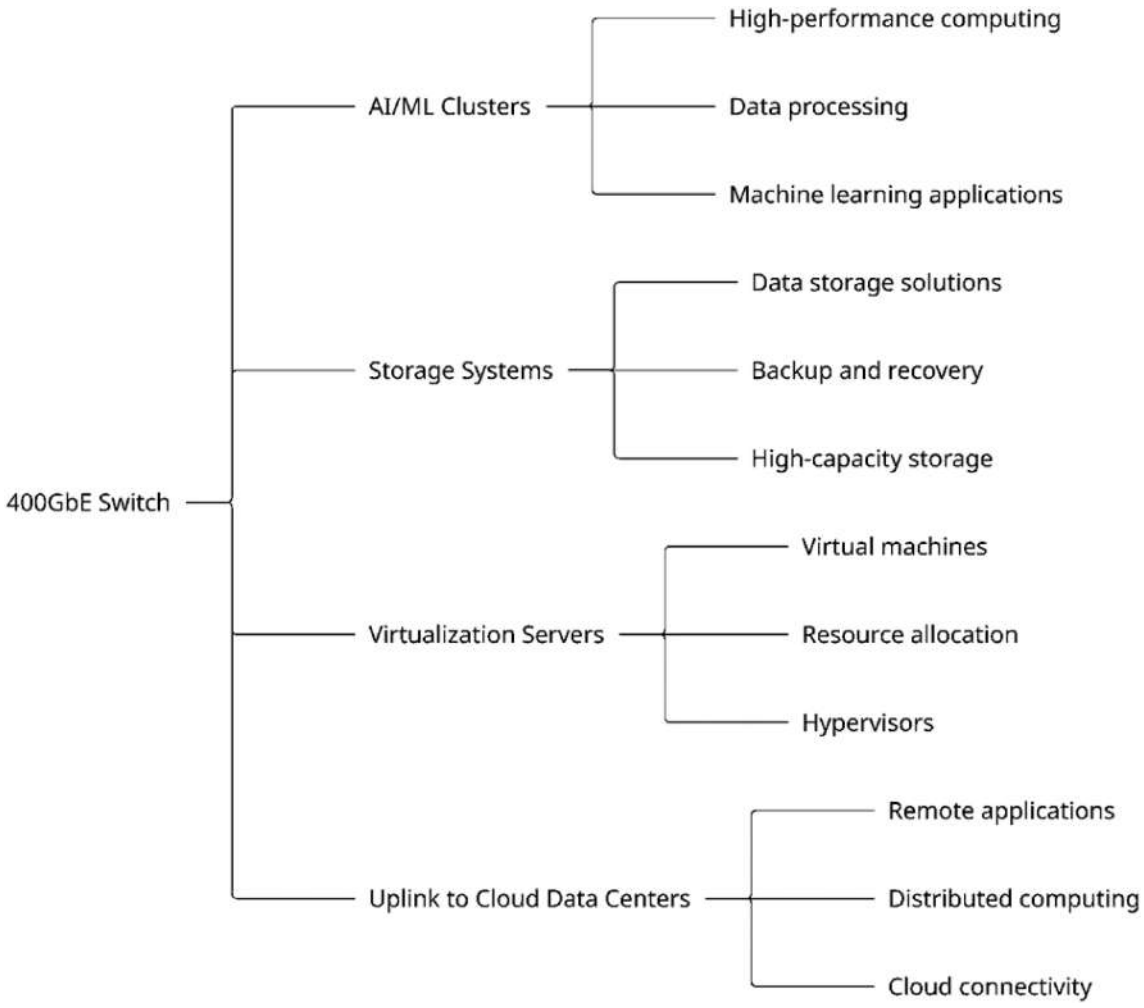

Fig. 7. Functional ecosystem enabled by a 400 GbE switch in modern data center infrastructure.

video streaming, virtual reality, and augmented reality is creating pressure for higher-speed networking infrastructure. Cloud service providers are among the early adopters of 400GbE technology, driven by the need to support increasing numbers of users and more demanding applications [78, 79]. The deployment of 400GbE requires comprehensive infrastructure planning and investment. Organizations must consider not only the cost of 400GbE switches and transceivers but also the associated infrastructure requirements including power, cooling, and physical space. The transition to 400GbE often requires upgrades to existing network infrastructure, including fiber optic cables, patch panels, and network management systems. Additionally, the deployment of 400GbE requires skilled personnel who understand the unique requirements and challenges of high-speed networking [80, 81]. Fig. 7 represents the depiction of a typical 400 Gigabit Ethernet deployment within a data center environment, showing connections between high-performance workloads, cloud uplinks, and distributed applications.

5.2. Network infrastructure evolution and upgrade strategies

The transition to higher-speed networking requires comprehensive infrastructure upgrades, including fiber optic cables, switching equipment, and network interface cards. This evolution represents a significant investment for organizations and requires careful planning to ensure compatibility and maximize return on investment. The upgrade to high-speed networking infrastructure is not simply a matter of replacing existing equipment but requires a holistic approach that considers all aspects of the network infrastructure [82, 83]. The fiber optic infrastructure required for high-speed networking has specific requirements that differ from traditional networking applications. High-speed applications require

high-quality fiber optic cables with low loss and dispersion characteristics. The installation of these cables requires specialized techniques and equipment to ensure optimal performance. Additionally, the connectors and patch panels used in high-speed networking must meet stringent performance requirements to maintain signal integrity and minimize insertion loss [84, 85]. The switching infrastructure required for high-speed networking incorporates advanced technologies that enable high-performance packet processing and switching. Modern high-speed switches use sophisticated packet processing engines that can handle millions of packets per second while maintaining low latency. These switches also incorporate advanced traffic management capabilities that can prioritize traffic based on application requirements and service level agreements. The implementation of these advanced switching capabilities requires sophisticated software and hardware architectures [86, 87]. The network interface cards (NICs) required for high-speed networking must be capable of handling the high data rates and low latency requirements of modern applications. Advanced NICs incorporate hardware acceleration capabilities that can offload processing tasks from the host CPU, improving overall system performance. These NICs also incorporate advanced error detection and correction capabilities that ensure reliable data transmission at high speeds. The selection and configuration of appropriate NICs is crucial for achieving optimal performance in high-speed networking environments [88, 89]. Fig. 8 is a visual breakdown of components required to upgrade to high-speed Ethernet infrastructure, from physical cabling to intelligent software-defined control layers.

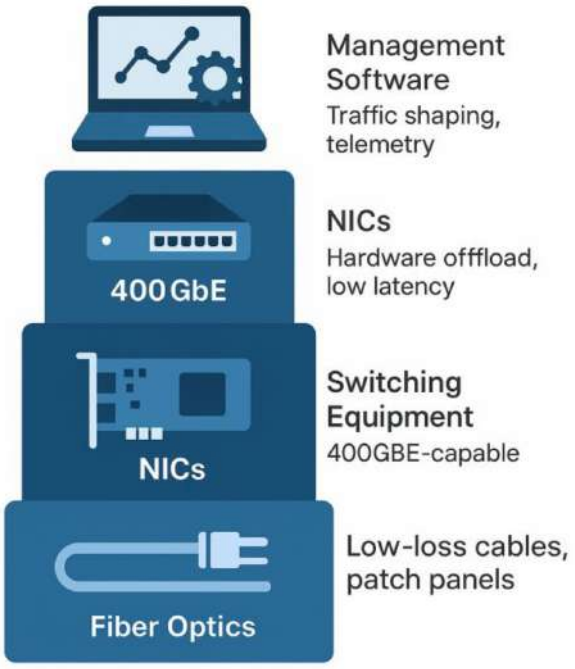

Fig. 8. High-speed networking upgrade stack.

5.3. Bandwidth and latency optimization for emerging applications

Emerging technologies such as virtual reality and augmented reality applications are driving demand for both increased bandwidth and reduced latency. Network designers must optimize for both parameters simultaneously to support these demanding applications effectively. This dual optimization presents significant challenges as traditional approaches to bandwidth and latency optimization can sometimes conflict with each other [90, 91]. The bandwidth requirements of emerging applications are substantial and continue to grow as applications become more sophisticated. Virtual reality applications require high-bandwidth connections to support the transmission of high-resolution video and audio content in real-time. Augmented reality applications have similar requirements but with the added complexity of overlaying digital content on real-world environments. The bandwidth requirements of these applications often exceed the capabilities of traditional networking infrastructure, requiring the deployment of high-speed networking technologies [92, 93]. The latency requirements of emerging applications are equally demanding and often more challenging to meet than bandwidth requirements. Virtual reality applications require extremely low latency to prevent motion sickness and provide immersive experiences. Augmented reality applications have similar requirements to ensure that digital overlays align properly with real-world environments. The achievement of ultra-low latency requires optimization at all levels of the network stack, from physical layer transmission to application-level processing [94, 95]. The optimization of networks for emerging applications requires sophisticated traffic engineering techniques that can balance bandwidth and latency requirements. Quality of service (QoS) mechanisms must be implemented to ensure that latency-sensitive traffic receives priority while maintaining fair access to bandwidth for other applications. Traffic shaping and buffering techniques must be carefully configured to minimize latency while preventing packet loss. Additionally, the implementation of advanced routing algorithms can help optimize path selection to minimize both latency and congestion [96, 97]. Table 5 summarizes the performance demands of emerging applications mapped against their bandwidth and latency sensitivities, along with suggested optimization techniques.

Table 5. Application bandwidth and latency requirements.

Application Type	Bandwidth Requirement	Latency Requirement	Typical Optimization Strategy
Virtual Reality (VR)	Very High (>1 Gbps)	Ultra Low (<20 ms)	Priority queuing, pre-buffering, local caching
Augmented Reality (AR)	High	Very Low (<30 ms)	Edge computing, fast routing
4K/8K Streaming	High	Moderate (<100 ms)	High-throughput uplinks, QoS shaping
AI/ML Data Training	Extremely High	Low	Dedicated 400GbE lanes, storage affinity

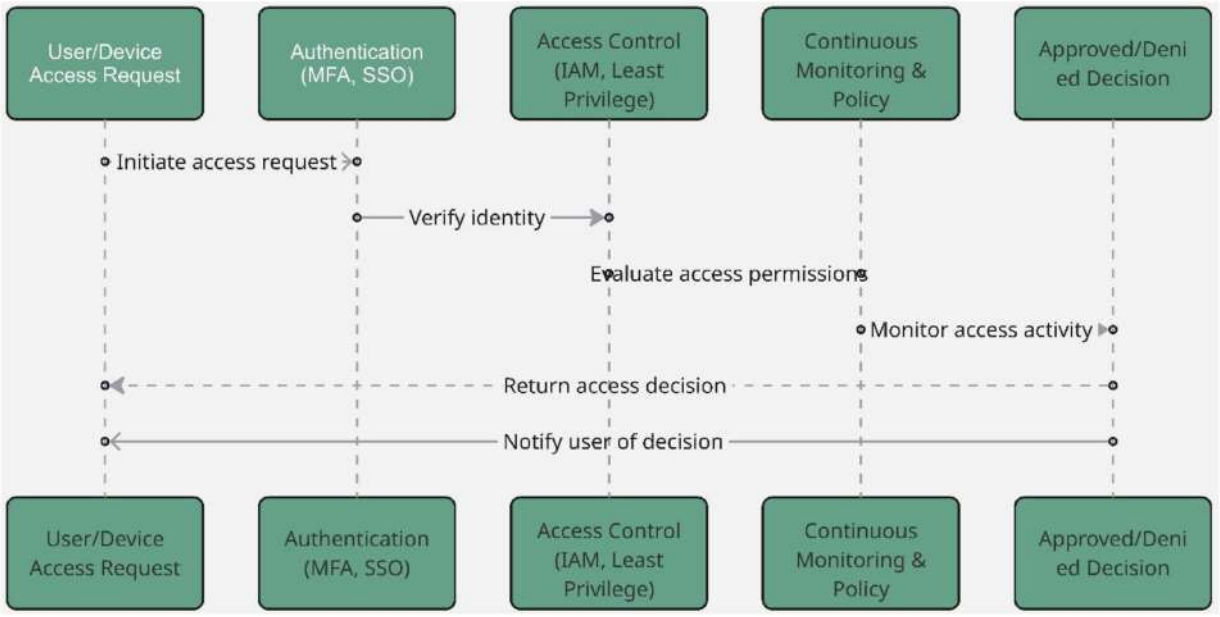

Fig. 9. Zero trust access control workflow for user and device authentication. A user or device initiates an access request, which is verified through authentication mechanisms such as multi-factor authentication (MFA) and single sign-on (SSO).

6. Security and zero trust architecture

6.1. Zero trust network security model

The zero trust security model assumes no implicit trust and requires verification for every access request, regardless of location (Fig. 9). This approach represents a fundamental shift from traditional perimeter-based security models that assumed internal network traffic could be trusted. The zero trust model recognizes that modern network environments are too complex and dynamic for traditional security approaches to be effective. With the proliferation of mobile devices, cloud services, and remote work, the traditional network perimeter has become increasingly porous and difficult to defend. As noted by Stafford (2020) in the NIST Special Publication, zero trust architecture (ZTA) is designed to protect resources based on identity and assets rather than network location [98]. Similarly, He et al. (2022) emphasize that ZTA offers a promising way to address modern challenges but remains in its early adoption phase, with implementation and awareness barriers still limiting its effectiveness [99]. Khan (2023) underscores that Zero Trust significantly reduces attack surfaces by enforcing granular segmentation and continuous monitoring [100], while Sarkar et al. (2022) highlight its potential to enhance cloud security by orchestrating intelligent, context-aware access control [101]. Collectively, these studies establish Zero Trust as a foundational paradigm for modern security.

The architectural foundation of zero trust networking rests on several key principles. First, the principle of "never trust, always verify" requires that all access requests be authenticated and authorized, regardless of the source location or previous authentication status. Second, the principle of least privilege access ensures that users and systems are granted only the minimum access required to perform their legitimate functions. Third, the principle of continuous monitoring and validation ensures that access permissions are constantly evaluated and adjusted based on changing conditions and risk factors. Assunção (2019) demonstrates that these principles align with the realities of cloud and IoT environments where user mobility and device proliferation weaken traditional perimeters [102]. Likewise, Edo et al. (2022) and Dhiman et al. (2024) provide comprehensive surveys showing that IAM, MFA, and dynamic micro-segmentation are core enablers for ZTA in practice [103, 104]. The

Table 6. Comparative analysis of core principles: Traditional security vs. zero trust security.

Principle	Traditional Security	Zero Trust Security
Trust Model	Implicit trust granted once inside the network perimeter, assuming internal entities are safe.	No implicit trust; every user, device, and application request is continuously verified regardless of location.
Perimeter Dependency	Strong reliance on physical or network perimeter (firewalls, VPNs) for defense.	Perimeter-less model; identity-, context-, and risk-aware access that adapts dynamically to conditions.
Access Control	Broad access once authenticated, leading to lateral movement risks within the network.	Least-privilege enforced per session; granular, policy-based access limits exposure and reduces attack surface.
Device/Identity Validation	Static, one-time login validation with limited post-authentication checks.	Continuous validation of device health, user identity, and behavioral patterns throughout the session.
Monitoring & Response	Intermittent, reactive monitoring; threats often detected post-compromise.	Continuous, proactive monitoring with automated detection and response, minimizing dwell time of attackers.
Adaptability & Scalability	Rigid architectures that struggle with cloud, mobile, and IoT integration.	Cloud-native, scalable, and adaptive to hybrid/multi-cloud environments and distributed workforces.
Security Philosophy	"Trust but verify" — assumes safety inside perimeter.	"Never trust, always verify" — assumes breach and designs controls accordingly.

conceptual roots of this approach are attributed to Kindervag (2010), who first proposed Zero Trust as a "never trust, always verify" strategy for designing security architectures "from the inside out" [105].

The network segmentation capabilities required for Zero Trust architecture are sophisticated and must be capable of creating granular security boundaries throughout the network. Traditional network segmentation approaches that rely on VLANs and firewalls are insufficient for Zero Trust environments. SDN and NFV technologies enable the implementation of micro-segmentation that can create boundaries at the application and workload level.

Beyond Zero Trust and microsegmentation, recent advances in privacy-preserving and intelligent security approaches are reshaping the field. In their seminal work, Yao (1982) introduced Secure Multi-Party Computation (SMPC), later expanded by Goldreich (2004), showing how multiple entities can jointly compute a function over private inputs without revealing the underlying data — a critical development for collaborative analytics in healthcare and finance. Similarly, Gentry (2009) pioneered Fully Homomorphic Encryption (FHE), demonstrating for the first time that arbitrary computations could be performed directly on encrypted data, thus enabling secure outsourcing of analytics to untrusted cloud providers while preserving confidentiality. More recent refinements by Halevi and Shoup (2014) improved the efficiency of such schemes, making them increasingly practical for real-world deployment. Parallel to these cryptographic innovations, Sommer and Paxson (2010) highlighted the limitations of traditional intrusion detection and argued for adaptive methods; more recently, Buczak and Guven (2016) surveyed machine learning-based intrusion detection systems (IDS), showing how AI techniques improve detection accuracy and adapt to novel attack vectors. Building on this, Ferrag et al. (2020) provided a systematic review of deep learning approaches for intrusion detection, demonstrating their effectiveness in handling high-volume, high-dimensional traffic data. Together, these contributions highlight that SMPC and homomorphic encryption address confidentiality and trust in distributed systems, while AI-driven IDS enhances proactive and adaptive defense capabilities.

By incorporating these complementary approaches Zero Trust, SMPC, homomorphic encryption, and AI-driven intrusion detection a more comprehensive security paradigm emerges. Zero Trust establishes strict access and micro-segmentation principles; SMPC and homomorphic encryption protect sensitive data during collaborative computation and outsourced analytics; and AI-IDS ensures continuous, intelligent threat detection. This holistic view responds to the increasing complexity of digital infrastructures and provides a forward-looking perspective on the convergence of cryptographic, architectural, and AI-driven security innovations.

Table 6 summarizes the comparison of fundamental security principles in traditional network security models versus modern Zero Trust architectures.

6.2. Network segmentation and microsegmentation

Advanced network segmentation techniques are being deployed to limit the potential impact of security breaches. Microsegmentation allows organizations to create granular security policies that restrict lateral movement within networks. This approach recognizes that traditional network security models, which focus on protecting the network perimeter, are insufficient for modern threat

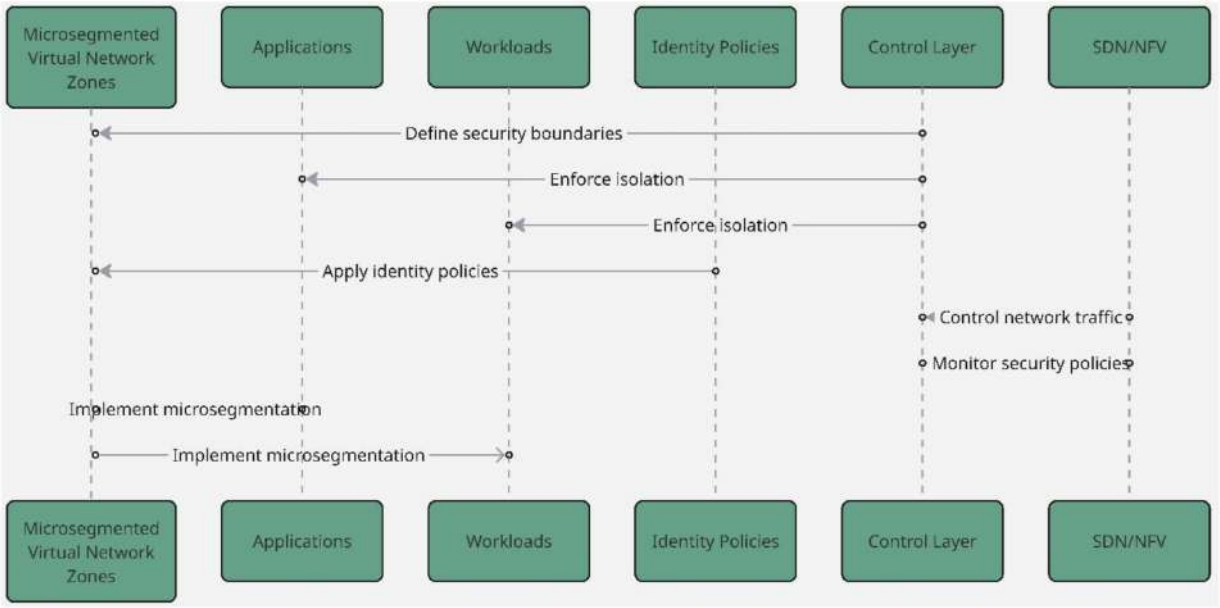

Fig. 10. Microsegmentation implementation model.

environments where attackers often gain initial access through social engineering, phishing, or other techniques that bypass perimeter defenses [106, 107]. The technological foundation of microsegmentation relies on several key capabilities that enable granular security policy enforcement. SDN provides the centralized control plane that can implement and enforce security policies across the network infrastructure. NFV enables the deployment of security functions such as firewalls and intrusion detection systems as software-based services that can be dynamically deployed and configured. Additionally, advanced monitoring and analytics capabilities are required to detect and respond to security threats within microsegmented environments [108, 109]. The implementation of microsegmentation requires comprehensive policy management capabilities that can define and enforce security policies at a granular level. Organizations must be able to define security policies based on various factors including user identity, device type, application requirements, and data sensitivity. These policies must be dynamically enforced across the network infrastructure, with the ability to adapt to changing conditions and requirements. The complexity of policy management in microsegmented environments requires sophisticated policy management tools and processes [110, 111]. The benefits of microsegmentation extend beyond simple security improvements to encompass compliance and operational efficiency benefits. By creating granular security boundaries, organizations can better control access to sensitive data and systems, improving compliance with regulatory requirements. Additionally, microsegmentation can improve incident response capabilities by limiting the scope of security breaches and providing more detailed visibility into network activity. The ability to isolate compromised systems quickly can significantly reduce the impact of security incidents [112, 113]. Fig. 10 illustrating microsegmentation architecture using SDN/NFV, where security policies enforce isolation of individual workloads and applications.

Table 7 summarizes a key difference between traditional segmentation techniques and microsegmentation in terms of granularity, flexibility, and enforcement.

6.3. Integrated security solutions and threat intelligence

Modern networks are incorporating security capabilities directly into network infrastructure rather than relying solely on separate security appliances. This integration provides better performance and more comprehensive protection by eliminating the bottlenecks and blind spots that can occur when security functions are implemented as separate, standalone systems. The integration of security capabilities into network infrastructure represents a fundamental shift in how organizations approach network security architecture [114, 115]. The technological foundation of integrated security solutions relies on several key capabilities that enable seamless integration of security functions into network infrastructure. Hardware-based security acceleration provides the processing power required to implement

Table 7. Network segmentation vs. microsegmentation.

Attribute	Traditional Segmentation	Microsegmentation
Scope	VLANs/Subnets	Per workload, per application
Technology	Hardware-based (switches/firewalls)	Software-defined (SDN/NFV)
Flexibility	Static	Highly dynamic
Enforcement Level	Network level	Application, identity, or workload level
Response Speed	Manual reconfiguration	Automated, real-time enforcement

sophisticated security functions without impacting network performance. Software-defined security capabilities enable the dynamic deployment and configuration of security functions based on changing requirements and threat conditions. Additionally, advanced threat intelligence capabilities provide the real-time threat information required to implement effective security policies and responses [116, 117]. The implementation of integrated security solutions requires sophisticated orchestration and management capabilities that can coordinate security functions across the network infrastructure. Security policies must be consistently applied across all network components, with the ability to adapt to changing conditions and requirements. This requires centralized security management platforms that can provide unified visibility and control over all security functions. Additionally, the integration of security functions with network operations requires new operational procedures and skills [118, 119]. The benefits of integrated security solutions are significant and multifaceted. By integrating security functions into network infrastructure, organizations can achieve better performance and more comprehensive protection than traditional approaches. The elimination of security bottlenecks can improve overall network performance while providing more consistent security coverage. Additionally, integrated security solutions can provide better visibility into network activity and more effective incident response capabilities [120, 121]. Fig. 11 is a model of integrated security showing how security functions are embedded across network layers, supported by orchestration and real-time threat intelligence.

7. Sustainability and green networking

7.1. Energy efficiency and carbon footprint reduction

Network operators are increasingly focusing on energy efficiency to reduce operational costs and environmental impact. This focus on sustainability represents a fundamental shift in how organizations approach network design and operation, moving from purely performance-focused approaches to more holistic strategies that consider environmental impact alongside technical requirements. The networking industry is a significant consumer of energy, with data centers and network infrastructure accounting for a substantial portion of global energy consumption [122, 123]. The technological foundation of energy-efficient networking relies on several key strategies that can significantly reduce power consumption without compromising performance. Advanced power management capabilities enable network equipment to dynamically adjust power consumption based on traffic load and utilization patterns. This includes the implementation of sleep modes for unused ports and interfaces, dynamic frequency scaling for processors, and intelligent cooling systems that adjust to actual thermal loads. Additionally, the development of more efficient hardware architectures, including advanced semiconductor technologies and optimized circuit designs, can significantly reduce power consumption [124, 125]. The implementation of energy-efficient networking requires comprehensive monitoring and management capabilities that can track energy consumption and identify optimization opportunities. Organizations must implement energy monitoring systems that can provide detailed visibility into power consumption at the device, system, and facility level. This information can be used to identify inefficient equipment, optimize power management settings, and plan energy-efficient upgrades. Additionally, the implementation of intelligent power management systems can automatically optimize power consumption based on traffic patterns and utilization requirements [126, 127]. The benefits of energy-efficient networking extend beyond simple cost reduction to encompass significant environmental and operational benefits. By reducing energy consumption, organizations can significantly reduce their carbon footprint and contribute to environmental sustainability goals. Additionally, energy-efficient networking can improve operational reliability by reducing heat generation and thermal stress on equipment. The reduced cooling requirements associated with energy-efficient networking can also provide additional cost savings and environmental benefits [128, 129]. Fig. 12 represents a high-level architecture of energy-efficient networking,

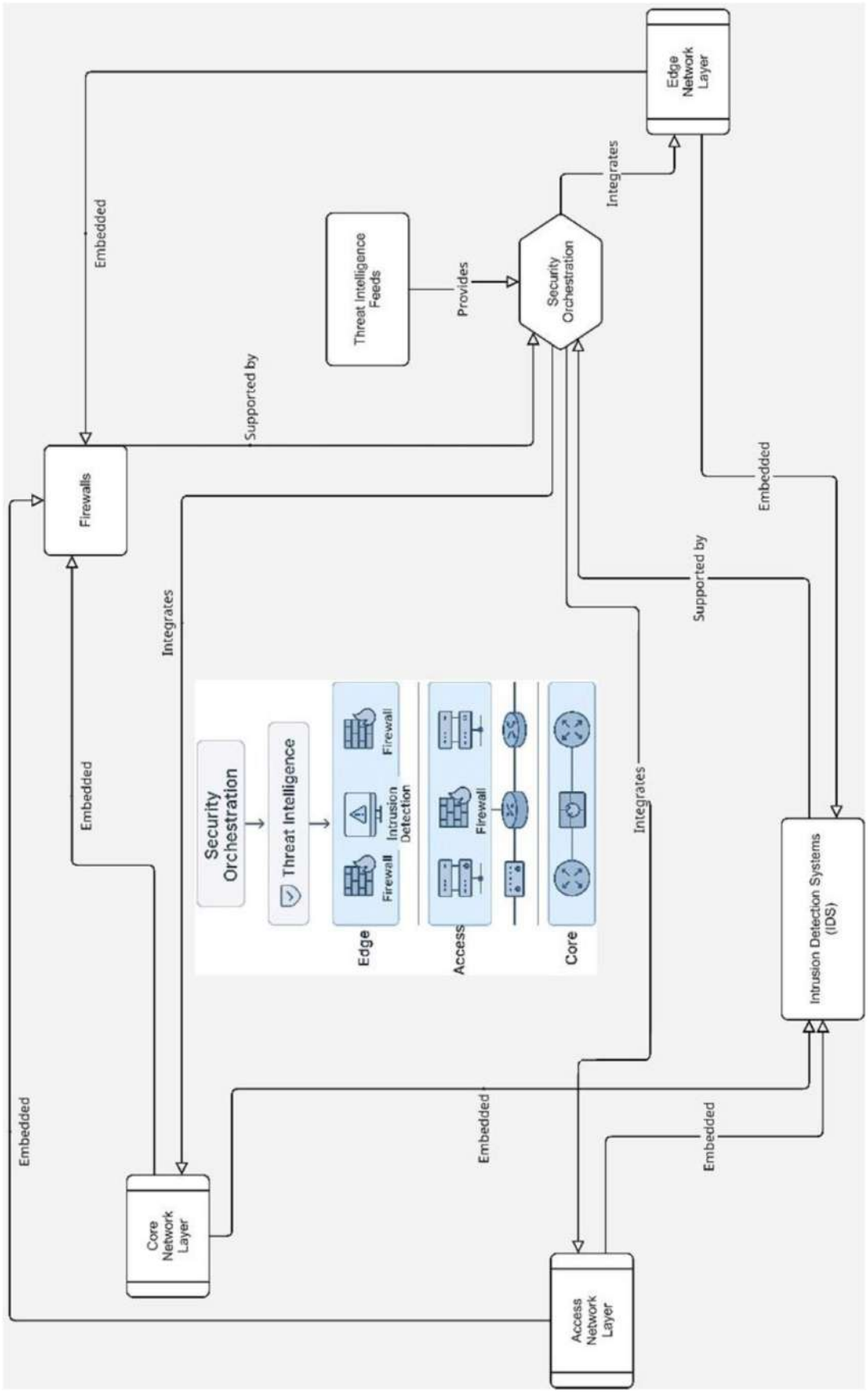

Fig. 11. Integrated security infrastructure model.

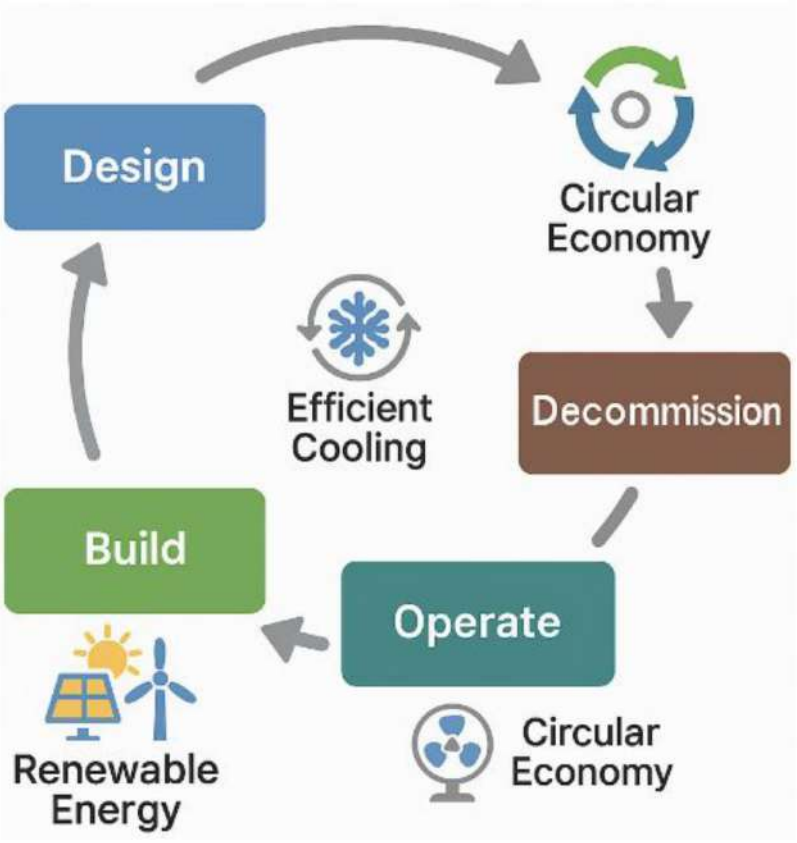

Fig. 12. Energy-efficient networking architecture.

Table 8. Energy optimization techniques in networking equipment.

Technique	Function	Impact
Sleep Mode for Ports/Links	Shuts down unused interfaces	Reduces idle power usage
Dynamic Frequency Scaling	Adjusts processor speed based on load	Balances performance and energy savings
Energy-Efficient Ethernet (EEE)	Reduces power during low network activity	Optimized power during idle transmission
Thermal-Aware Cooling	Adjusts cooling systems to real-time heat load	Improves cooling efficiency
Low-Power Hardware Design	Uses advanced semiconductors and chipsets	Reduces overall device-level power draw

showing how traffic-aware power management, real-time monitoring, and optimization logic reduce energy consumption and carbon footprint.

Table 8 summarizes a common techniques and technologies used to optimize energy consumption in modern networking equipment, contributing to operational efficiency and sustainability.

7.2. Sustainable infrastructure design and renewable energy integration

New network designs prioritize sustainability through the use of renewable energy sources, efficient cooling systems, and equipment lifecycle management. These approaches help organizations meet environmental goals while maintaining network performance. The integration of sustainability considerations into network design requires a holistic approach that considers the entire lifecycle of network infrastructure, from initial design and deployment through operation and eventual decommissioning [130, 131]. The architectural foundation of sustainable network design incorporates several key principles that distinguish it from traditional approaches. First, the optimization of infrastructure efficiency through careful design and component selection can significantly reduce resource consumption and environmental impact. Second, the integration of renewable energy sources such as solar, wind, and hydroelectric power can reduce reliance on fossil fuels and decrease carbon emissions. Third, the implementation of circular economy principles through equipment reuse, recycling, and responsible disposal can minimize waste and resource consumption [132,

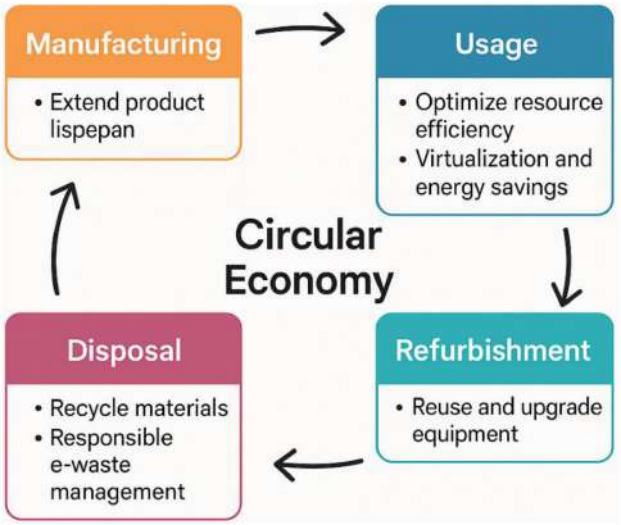

Fig. 13. Network equipment lifecycle and circular economy.

133]. The implementation of sustainable network design requires comprehensive planning and evaluation capabilities that can assess the environmental impact of different design options. Organizations must consider factors such as energy consumption, carbon emissions, material usage, and waste generation throughout the lifecycle of network infrastructure. This requires sophisticated modeling and analysis tools that can evaluate the environmental impact of different design choices and identify optimization opportunities. Additionally, the implementation of sustainable design principles requires collaboration with suppliers and partners to ensure that sustainability considerations are integrated throughout the supply chain [134, 135]. The benefits of sustainable network design are significant and multifaceted. By prioritizing sustainability, organizations can reduce their environmental impact while potentially achieving cost savings through improved efficiency and reduced resource consumption. Additionally, sustainable network design can improve organizational reputation and help meet corporate sustainability goals and regulatory requirements. The long-term benefits of sustainable design include reduced operational costs, improved equipment reliability, and enhanced resilience to environmental and regulatory changes [136, 137]. Fig. 13 visualizing a circular economy model in network lifecycle management, where proactive monitoring, modular design, and responsible disposal contribute to sustainable infrastructure.

Table 9 summarizes a comparison of environmental and operational characteristics between traditional and sustainability-driven network design strategies.

7.3. Lifecycle management and circular economy principles

Organizations are implementing comprehensive strategies to reduce their network-related carbon footprint, including virtualization to reduce hardware requirements, optimized routing to minimize energy consumption, and renewable energy adoption. The implementation of lifecycle management principles enables organizations to maximize the value and minimize the environmental impact of network infrastructure throughout its operational lifetime. This includes strategies for extending equipment lifecycles, optimizing resource utilization, and implementing responsible disposal and recycling practices [138, 139]. The technological foundation of lifecycle management relies on several key capabilities that enable effective management of network infrastructure throughout its operational lifetime. Advanced monitoring and analytics capabilities provide visibility into equipment performance, utilization, and health, enabling organizations to optimize maintenance schedules and extend equipment lifecycles. Predictive analytics capabilities can identify potential equipment failures before they occur, enabling proactive maintenance that can extend equipment life and reduce waste. Additionally, the implementation of modular and upgradeable equipment designs can enable incremental improvements and upgrades without requiring complete equipment replacement [140, 141]. The implementation of lifecycle management requires comprehensive planning and tracking capabilities that can monitor equipment throughout its operational lifetime. Organizations must maintain detailed records of equipment acquisition, deployment, maintenance, and performance to enable effective lifecycle management decisions. This information can be used to optimize maintenance schedules, plan upgrades and replacements, and implement responsible disposal practices. Additionally, the implementation of asset management systems can provide automated tracking and reporting capabilities that reduce administrative overhead and improve decision-making [142, 143]. The benefits of effective lifecycle management extend beyond environmental benefits to encompass significant cost savings and operational improvements. By extending equipment lifecycles and optimizing resource utilization, organizations can reduce capital and operational expenses while minimizing environmental impact. Additionally, effective lifecycle management can improve equipment reliability and performance by ensuring that equipment is properly maintained and operated within optimal parameters. The implementation of responsible disposal and recycling practices can also provide cost savings

Table 9. Environmental impact comparison – traditional vs. sustainable design.

Factor	Traditional Design	Sustainable Design
Power Source	Grid/Fossil-based	Solar/Wind/Hydro
Cooling Method	Air conditioning	Liquid cooling/Smart thermal systems
Hardware Lifecycle	Fixed, periodic replacement	Modular, upgradable, extended lifecycle
Material Waste	High	Reduced via recycling and reuse policies
Emission Impact	High CO_2 output	Reduced emissions with clean energy

Table 10. Lifecycle optimization techniques and benefits.

Technique	Description	Sustainability & Business Benefit
Predictive Maintenance	Uses analytics to prevent hardware failure	Extends device life, reduces e-waste
Modular Hardware Design	Enables partial upgrades without full replacement	Reduces material use and cost
Asset Tracking and Inventory	Real-time lifecycle and location tracking	Improves reuse, simplifies audits
Virtualization	Reduces physical infrastructure needs	Saves power and hardware
Certified Recycling Programs	Ensures responsible equipment disposal	Meets regulations, avoids landfill waste

and help organizations meet regulatory requirements [144, 145]. Table 10 summarizes a breakdown of best practices in network infrastructure lifecycle management, highlighting their impact on both environmental goals and operational performance.

8. Multi-cloud and hybrid cloud networking

8.1. Cloud-native networking architecture

The shift toward cloud-native applications requires networking solutions that can seamlessly span multiple cloud environments. This includes implementing consistent security policies, optimizing performance across clouds, and managing complex routing requirements. Cloud-native networking represents a fundamental shift from traditional enterprise networking models to more flexible, scalable architectures that can adapt to the dynamic requirements of modern applications and services [146, 147]. The architectural foundation of cloud-native networking relies on several key principles that distinguish it from traditional networking approaches. First, the abstraction of network services from underlying infrastructure enables applications to consume network resources without requiring knowledge of the underlying implementation details. Second, the implementation of declarative network policies allows applications to specify their networking requirements, with the underlying infrastructure automatically configuring the necessary resources. Third, the integration of networking capabilities with application lifecycle management enables network resources to be provisioned, configured, and deprovisioned automatically as applications are deployed and scaled [148, 149]. The implementation of cloud-native networking requires sophisticated orchestration and management capabilities that can coordinate network resources across multiple cloud environments. Organizations must implement network orchestration platforms that can provide unified visibility and control over network resources across different cloud providers and deployment models. This includes the ability to implement consistent security policies, optimize performance across different cloud environments, and manage complex routing requirements. Additionally, the implementation of cloud-native networking requires new operational procedures and skills that can effectively manage dynamic, software-defined network environments [150, 151]. The benefits of cloud-native networking are significant and enable organizations to leverage the full benefits of cloud computing while maintaining network performance and security. By abstracting network services from underlying infrastructure, organizations can achieve greater flexibility and agility in deploying and managing applications. The ability to implement consistent policies across multiple cloud environments simplifies security management and ensures compliance with organizational requirements. Additionally, cloud-native networking can improve application performance by optimizing network resources based on application requirements and usage patterns [152, 153]. Fig. 14 represents a layered model of cloud-native networking architecture showing the interaction between applications, policy-driven orchestration, and abstracted network services for seamless multi-cloud operations.

Table 11 summarizes the comparison of traditional enterprise networking models with modern cloud-native architectures across key operational and technical dimensions.

8.2. Hybrid infrastructure management and connectivity

Organizations are adopting hybrid approaches that combine on-premises infrastructure with multiple

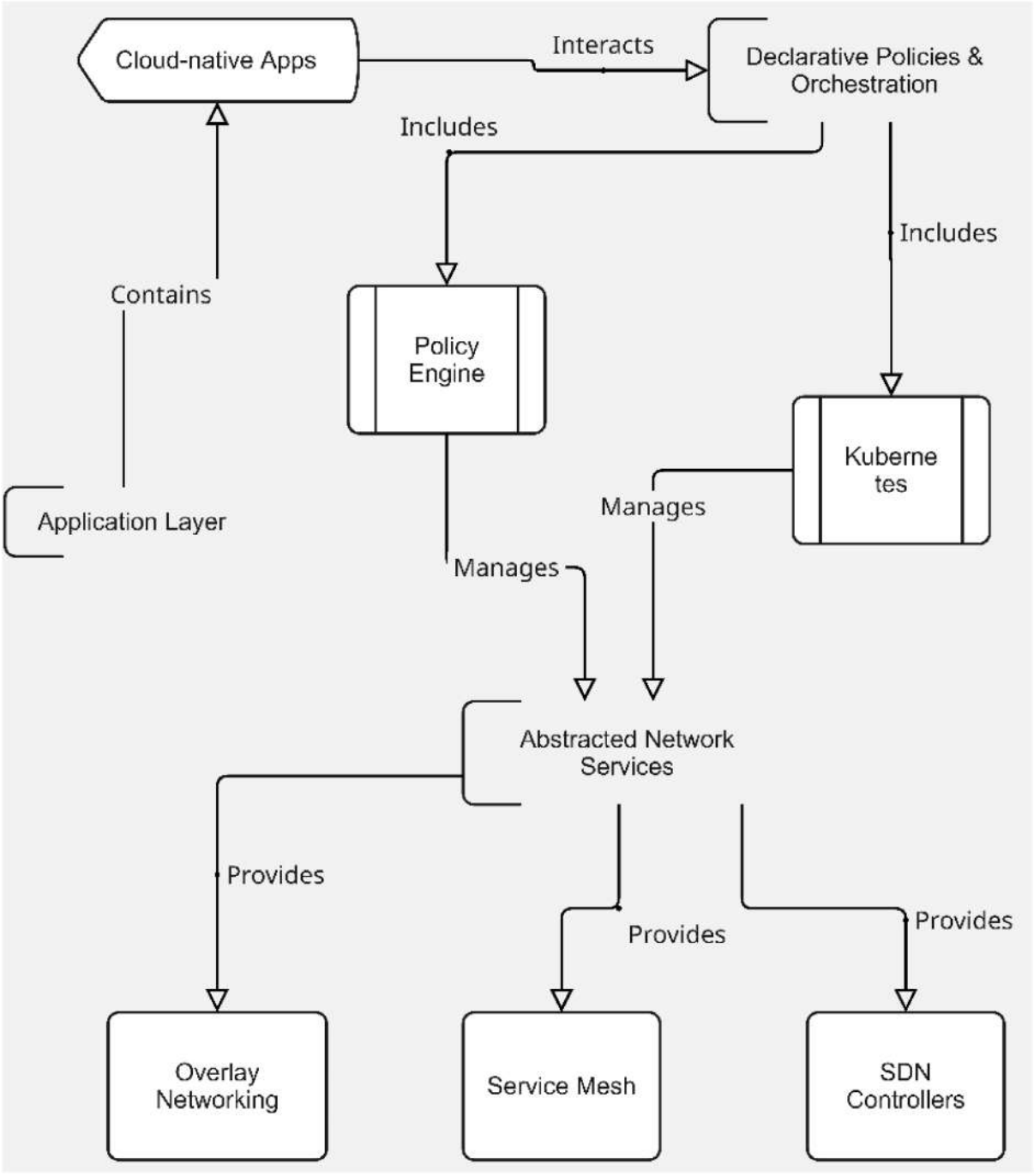

Fig. 14. Cloud-native networking architecture model.

Table 11. Comparison – traditional vs. cloud-native networking.

Feature	Traditional Networking	Cloud-Native Networking
Network Configuration	Manual, CLI-based	Declarative, automated
Infrastructure Dependency	Tightly coupled	Abstracted and decoupled
Policy Management	Static firewall rules	Dynamic, policy-as-code
Application Deployment	Static	Containerized, dynamic scaling
Lifecycle Integration	Limited	Fully integrated with CI/CD

Table 12. Key technologies in hybrid cloud networking.

Technology	Role in Hybrid Networking	Example Providers
SD-WAN	Optimized multi-site cloud connectivity	Cisco Viptela, VMware SD-WAN
NFV	Virtualized network services in hybrid deployment	Fortinet, Palo Alto, F5
Hybrid Orchestration	Unified visibility and control across environments	HashiCorp Terraform, Red Hat ACM
Monitoring/Analytics	Performance and anomaly detection	Datadog, Prometheus, Splunk

cloud providers. This strategy requires sophisticated networking solutions that can manage connectivity, security, and performance across diverse environments. Hybrid infrastructure represents a pragmatic approach to cloud adoption that enables organizations to leverage the benefits of cloud computing while maintaining control over sensitive data and applications that may be better suited to on-premises deployment [154, 155]. The architectural foundation of hybrid infrastructure management relies on several key capabilities that enable seamless integration between on-premises and cloud environments. Software-defined WAN (SD-WAN) technology provides the networking foundation that can optimize connectivity between on-premises and cloud resources while maintaining security and performance. NFV enables the deployment of network services such as firewalls, load balancers, and intrusion detection systems across hybrid environments. Additionally, advanced monitoring and analytics capabilities provide visibility into performance and security across all components of the hybrid infrastructure [156, 157]. The implementation of hybrid infrastructure management requires comprehensive orchestration and management capabilities that can coordinate resources across different environments and providers. Organizations must implement hybrid cloud management platforms that can provide unified visibility and control over all components of the hybrid infrastructure. This includes the ability to implement consistent security policies, optimize performance across different environments, and manage complex routing and connectivity requirements. The complexity of hybrid infrastructure management requires sophisticated automation capabilities that can handle the dynamic nature of cloud environments while maintaining consistency and reliability across all components [158, 159]. Table 12 is a key enabling technologies and vendor examples for implementing resilient, secure hybrid cloud network architectures.

8.3. Inter-cloud connectivity and performance optimization

As organizations utilize multiple cloud providers, the need for efficient inter-cloud connectivity becomes critical. Direct connection services and optimized routing protocols are essential for maintaining performance across distributed cloud environments. The implementation of multi-cloud strategies introduces significant networking challenges that must be addressed through sophisticated connectivity solutions and performance optimization techniques [160, 161]. The technological foundation of inter-cloud connectivity relies on several key capabilities that enable efficient communication between different cloud providers. Direct connection services such as AWS Direct Connect, Azure ExpressRoute, and Google Cloud Interconnect provide dedicated, high-bandwidth connections between on-premises infrastructure and cloud providers. These services bypass the public internet, providing more predictable performance and enhanced security. Additionally, cloud-to-cloud connectivity services enable direct connections between different cloud providers, reducing latency and improving performance for multi-cloud applications [162, 163]. The implementation of inter-cloud connectivity requires careful planning and optimization to ensure optimal performance and cost-effectiveness. Organizations must evaluate different connectivity options based on factors such as bandwidth requirements, latency sensitivity, security requirements, and cost considerations. The selection of appropriate connectivity services and configurations can significantly impact application performance and operational costs. Additionally, the implementation of intelligent routing protocols can optimize traffic flow across multiple cloud environments, ensuring that applications utilize the most efficient paths for different types of traffic [164, 165]. The benefits of optimized inter-cloud connectivity extend beyond simple performance improvements to encompass significant operational and strategic benefits. By implementing efficient connectivity between cloud providers, organizations can achieve better application performance, reduced latency, and improved user experience. Additionally, optimized inter-cloud connectivity can enable more sophisticated multi-cloud architectures that can leverage the unique capabilities of different cloud providers while maintaining seamless integration and consistent performance [166, 167]. Table 13 summarizes the comparison of common inter-cloud connectivity options highlighting latency, cost, and ideal application scenarios.

Table 13. Inter-cloud connectivity options and trade-offs.

Connectivity Option	Latency	Bandwidth	Security	Cost	Best Use Case
Public Internet	High	Variable	Low	Low	Low-sensitivity, non-critical traffic
VPN over Internet	Medium	Medium	Medium	Moderate	Quick secure connection
Direct Cloud Connection	Low	High	High	High	Critical business traffic
Cloud-to-Cloud Peering	Very Low	High	High	Varies	Latency-sensitive multi-cloud apps

9. Future outlook and emerging technologies

9.1. IPv6 migration and next-generation internet protocol

The transition to IPv6 is accelerating as IPv4 address exhaustion becomes more pressing, with organizations implementing dual-stack configurations and planning comprehensive migration strategies to ensure continuity during the transition period. The migration to IPv6 represents one of the most significant changes in internet infrastructure since the original deployment of the Internet Protocol, affecting virtually every aspect of network design, operation, and security. This transition is not merely a technical upgrade but a fundamental shift that will enable new capabilities and applications while addressing the scalability limitations of IPv4 [169]. The technological foundation of IPv6 provides significant advantages over IPv4 that extend far beyond simple address space expansion. The 128-bit address space of IPv6 provides virtually unlimited addressing capacity, enabling the connection of billions of devices without the need for network address translation (NAT) and other workarounds required by IPv4. The simplified header structure of IPv6 improves routing efficiency and reduces processing overhead, potentially improving network performance. Additionally, IPv6 includes built-in support for features such as auto-configuration, quality of service, and security that were added to IPv4 through extensions and additional protocols [170]. The implementation of IPv6 migration requires comprehensive planning and execution strategies that address the complexity of transitioning existing networks and applications. Organizations must develop detailed migration plans that consider factors such as application compatibility, network infrastructure requirements, security implications, and operational procedures. The migration process typically involves implementing dual-stack configurations that support both IPv4 and IPv6 simultaneously, allowing for gradual transition while maintaining backward compatibility. Additionally, the implementation of translation mechanisms enables communication between IPv4 and IPv6 networks during the transition period [171]. The challenges associated with IPv6 migration are significant and multifaceted, requiring careful planning and execution to ensure successful transition. Application compatibility represents one of the most significant challenges, as many existing applications were designed specifically for IPv4 and may require modification or replacement to support IPv6. Network infrastructure components such as routers, switches, and firewalls must be upgraded or replaced to support IPv6 functionality. Additionally, operational procedures and staff training must be updated to address the unique requirements of IPv6 networks [172]. The benefits of IPv6 migration extend beyond simple address space expansion to encompass significant improvements in network functionality and efficiency. The elimination of NAT requirements simplifies network architecture and improves application performance by enabling true end-to-end connectivity. The built-in security features of IPv6 provide enhanced protection against various types of attacks, while the improved routing efficiency can reduce network latency and improve overall performance. Additionally, the virtually unlimited address space of IPv6 enables new applications and services that were not feasible with IPv4 [173]. Looking toward the future, IPv6 migration will continue to accelerate as IPv4 address exhaustion becomes more severe and the benefits of IPv6 become more apparent. Organizations that proactively plan and execute IPv6 migration will be better positioned to support future growth and take advantage of new capabilities enabled by IPv6. The transition to IPv6 will also enable the development of new applications and services that leverage the unique capabilities of the next-generation internet protocol.

9.2. Quantum-safe networking and post-quantum cryptography

Preparation for quantum computing's impact on network security is beginning, with organizations evaluating quantum-safe cryptographic algorithms and planning infrastructure upgrades to protect against future quantum-based attacks. The development of practical quantum computers poses a significant threat to current cryptographic systems, as quantum algorithms such as Shor's algorithm can efficiently break the mathematical foundations of widely used public-key cryptography systems. This

threat requires proactive preparation and implementation of quantum-safe cryptographic solutions to maintain network security in the post-quantum era [174]. The technological foundation of quantum-safe networking relies on cryptographic algorithms that are believed to be resistant to attacks by quantum computers. These algorithms, collectively known as post-quantum cryptography (PQC), are based on mathematical problems that are thought to be difficult for both classical and quantum computers to solve. The National Institute of Standards and Technology (NIST) has been conducting a multi-year process to evaluate and standardize post-quantum cryptographic algorithms, with several algorithms already selected for standardization. These algorithms include lattice-based, code-based, multivariate, and hash-based cryptographic systems [175]. Quantum-safe networking demands evaluating and deploying post-quantum cryptographic algorithms, assessing current implementations, planning migration, and addressing performance impacts from larger key sizes and increased computational requirements across network components. Additionally, the implementation of crypto-agility principles enables organizations to quickly adapt to new cryptographic standards as they are developed and deployed [176]. The challenges associated with quantum-safe networking are significant and require careful planning and execution. The performance implications of post-quantum algorithms can be substantial, with some algorithms requiring significantly more computational resources and larger key sizes than current algorithms. This can impact network performance and require hardware upgrades to maintain acceptable performance levels. Additionally, the interoperability challenges associated with deploying new cryptographic algorithms across diverse network environments require careful coordination and testing [177]. The timeline for quantum-safe networking implementation is driven by the progress in quantum computing development and the maturity of post-quantum cryptographic standards. While large-scale, cryptographically relevant quantum computers do not currently exist, the rapid pace of quantum computing research suggests that such systems may be available within the next 10-20 years. Organizations must begin planning and implementing quantum-safe networking solutions now to ensure that they are prepared for the post-quantum era. The transition to quantum-safe networking will likely require several years to complete, making early preparation essential [178]. The benefits of quantum-safe networking extend beyond simple protection against quantum attacks to encompass improvements in overall cryptographic security and resilience. By implementing quantum-safe algorithms, organizations can protect their networks against both current and future threats, ensuring long-term security and compliance. The proactive implementation of quantum-safe networking will provide organizations with a competitive advantage and enhanced security posture in the post-quantum era [179]. Fig. 15 illustrating the foundational elements of quantum-safe networking. It highlights the core relationship between emerging quantum threats and corresponding countermeasures such as post-quantum cryptographic algorithms and resistant key exchange protocols key strategies for securing networks in the post-quantum era.

9.3. Autonomous network operations and self-healing systems

The development of fully autonomous networks that can self-configure, self-optimize, and self-heal represents the next frontier in network evolution. These systems will leverage advanced AI and ML to operate with minimal human intervention, fundamentally transforming how networks are designed, deployed, and managed. Autonomous networking represents the convergence of multiple technologies including AI, ML, software-defined networking, and advanced analytics to create networks that can adapt and respond to changing conditions without human intervention [180]. The technological foundation of autonomous networking relies on several key capabilities that enable self-managing network systems. Advanced ML algorithms can analyze network behavior, identify patterns, and make intelligent decisions about network configuration and optimization. Predictive analytics capabilities can anticipate network issues and proactively implement solutions before problems occur. Additionally, sophisticated automation frameworks can implement configuration changes, deploy new services, and respond to incidents without human intervention. The integration of these capabilities creates network systems that can continuously optimize their performance and adapt to changing requirements [181]. The implementation of autonomous networking requires comprehensive data collection and analysis capabilities that can provide the information needed for intelligent decision-making. Networks must be instrumented with sensors and monitoring systems that can collect detailed information about network performance, traffic patterns, and system health. This data must be processed and analyzed in real-time to enable immediate response to changing conditions. Additionally, the implementation of digital twin technologies can create virtual models of network infrastructure that can be used for testing and optimization without

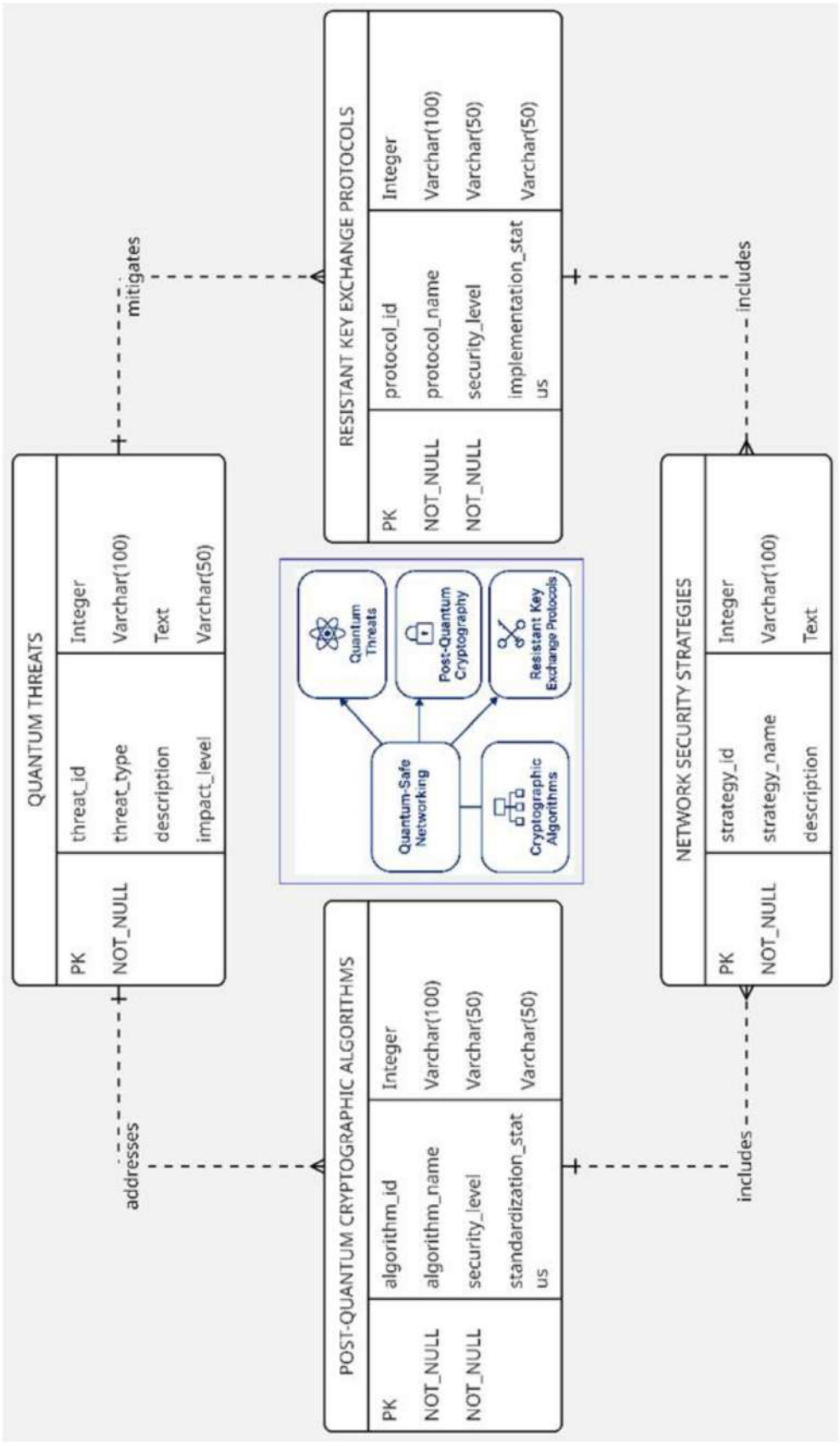

Fig. 15. Quantum-safe networking and post-quantum cryptography.

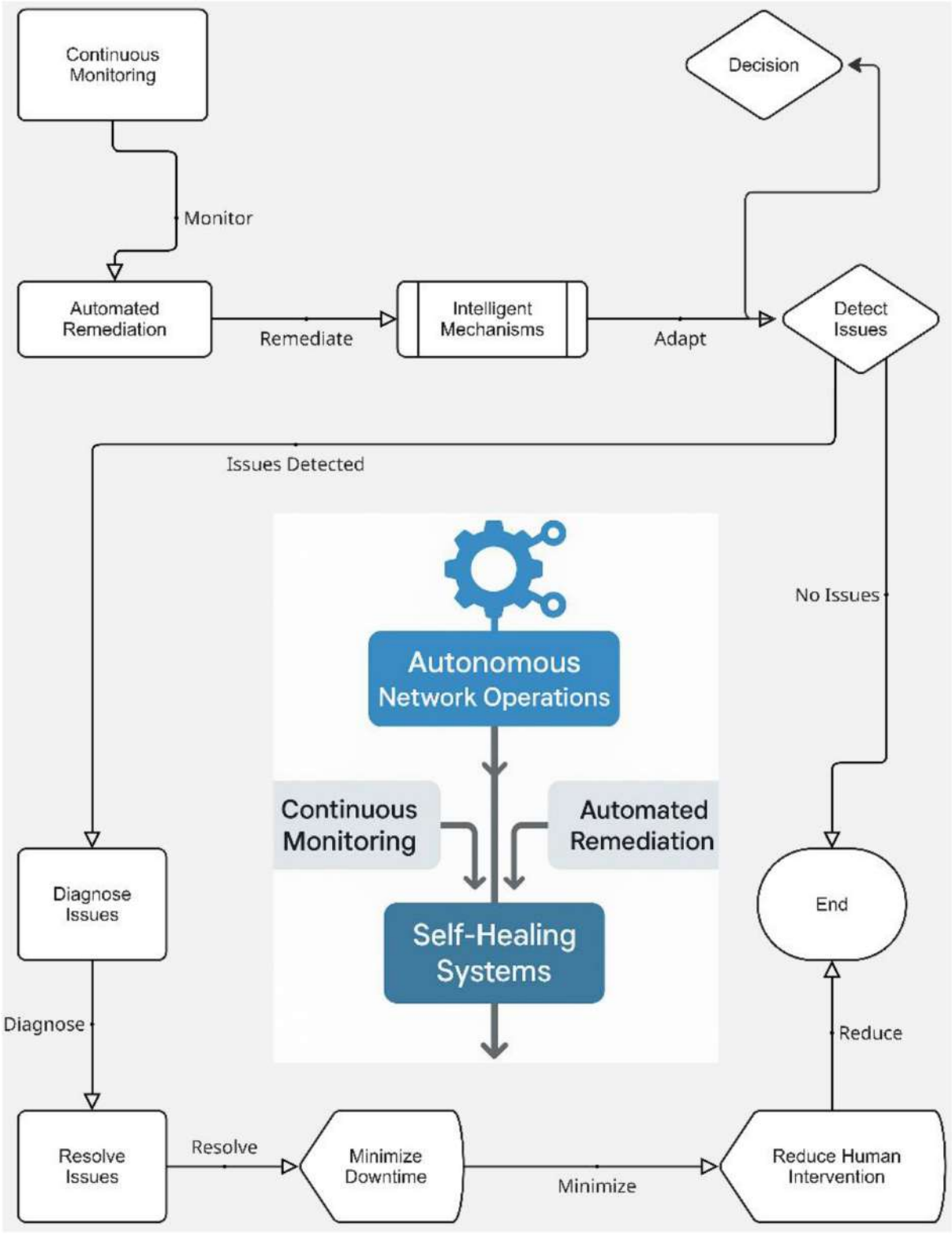

Fig. 16. Autonomous network operations through self-healing systems.

impacting production systems [182]. The benefits of autonomous networking are significant and have the potential to transform network operations fundamentally. By eliminating the need for manual configuration and management, autonomous networks can reduce operational costs and improve efficiency. The ability to continuously optimize network performance can improve application performance and user experience while reducing resource consumption. Additionally, autonomous networks can improve reliability by quickly identifying and resolving issues before they impact users. The self-healing capabilities of autonomous networks can significantly reduce downtime and improve overall system availability [183]. The challenges associated with autonomous networking are substantial and require careful consideration during implementation. The complexity of autonomous systems can make them difficult to understand, troubleshoot, and maintain. Organizations must develop new skills and procedures for managing autonomous networks, including the ability to monitor and validate autonomous decisions. Additionally, the security implications of autonomous networks must be carefully considered, as these systems may be vulnerable to new types of attacks that exploit their autonomous capabilities [184]. The evolution toward autonomous networking will likely occur gradually, with organizations implementing increasingly sophisticated automation capabilities over time. Early implementations may focus on specific use cases such as traffic optimization, fault detection, and capacity planning. As the technology matures and organizations gain experience with autonomous systems, more comprehensive autonomous networking capabilities will be deployed. The ultimate goal is to create networks that can operate independently while maintaining the flexibility to adapt to changing business requirements and technological developments. Fig. 16 illustrating the key components of autonomous network operations enabled by self-healing systems. The process begins with continuous monitoring and automated remediation, feeding into intelligent, adaptive mechanisms that detect, diagnose, and resolve network issues in real time minimizing downtime and reducing human intervention.

10. Conclusion and strategic recommendations

10.1. Conclusion

The convergence of artificial intelligence, edge computing, and advanced virtualization is propelling networks toward more intelligent, distributed, and autonomous architectures. These technologies are mutually reinforcing, offering scalability, agility, and performance improvements, while simultaneously raising new challenges in security, sustainability, and implementation complexity. A central finding of this review is that security must be embedded by design: Zero Trust architectures and emerging cryptographic approaches, such as quantum-safe methods, provide essential safeguards for dynamic, multi-layered environments. At the same time, sustainability requires deliberate planning to balance the energy demands of AI and edge infrastructures with efficiency gains from automation and optimization. Economically, organizations must recognize that although modern networking requires significant upfront investment in infrastructure and skills, these costs are offset by long-term benefits in operational efficiency and competitive differentiation.

To respond effectively, organizations should adopt phased implementation strategies that begin with controlled pilots and scale incrementally to reduce risks. Security frameworks must be integrated early, ensuring that authentication, continuous monitoring, and advanced cryptography form part of the network foundation rather than afterthoughts. Networking modernization should also align with sustainability goals through energy-efficient designs and adaptive workload distribution at the edge. Finally, investment in workforce development and skills readiness is critical, as the ability to operate and manage these complex infrastructures is as important as the technologies themselves. In sum, the future of networking will be defined not by individual innovations but by the strategic integration of multiple advancing technologies, with organizations that adopt holistic, secure, and sustainability-driven strategies best positioned to capture long-term value.

10.2. Key recommendations for organizations

Based on the analysis of current networking trends and their implications, several key recommendations emerge for organizations seeking to optimize their network infrastructure and capabilities. These recommendations provide a roadmap for leveraging emerging technologies while managing risks and ensuring successful implementation.

First, organizations should invest in AIOps capabilities that can provide intelligent monitoring, predictive analytics, and automated response capabilities. The implementation of AIOps platforms can significantly improve network reliability, reduce operational costs, and enable more efficient resource utilization. Organizations should begin by identifying specific use cases where AI can provide

immediate benefits, such as fault detection, performance optimization, and capacity planning. The gradual expansion of AI capabilities across network operations can provide increasing benefits over time.

Second, organizations should develop comprehensive edge computing strategies that align with their business requirements and technical capabilities. The implementation of edge computing can provide significant benefits for applications requiring low latency, high bandwidth, or local processing capabilities. Organizations should evaluate their application portfolios to identify candidates for edge deployment and develop detailed implementation plans that address connectivity, security, and management requirements. The integration of edge computing with existing cloud and on-premises infrastructure requires careful planning and execution to ensure optimal performance and cost-effectiveness.

Third, organizations should plan for high-speed connectivity upgrades that can support future growth and emerging applications. The transition to technologies such as 400 Gigabit Ethernet requires comprehensive infrastructure planning and investment. Organizations should develop detailed upgrade plans that consider factors such as bandwidth requirements, latency sensitivity, and budget constraints. The implementation of high-speed connectivity should be aligned with application requirements and business objectives to ensure optimal return on investment.

Fourth, organizations should implement comprehensive security frameworks based on zero trust principles. The increasing complexity and distributed nature of modern networks require security approaches that assume no implicit trust and verify all access requests. Organizations should develop detailed zero trust implementation plans that address identity management, network segmentation, and policy enforcement. The gradual implementation of zero trust capabilities can provide increasing security benefits while minimizing disruption to existing operations.

Fifth, organizations should prioritize sustainability considerations in network design and operation. The increasing focus on environmental sustainability requires organizations to consider the energy consumption and carbon footprint of their network infrastructure. Organizations should implement energy-efficient technologies, optimize power management, and consider renewable energy sources where feasible. The integration of sustainability considerations into network planning and operation can provide both environmental and economic benefits.

Finally, organizations should invest in skills development and training to ensure that their personnel can effectively manage and operate new networking technologies. The rapid pace of technological change requires ongoing investment in skills development to maintain competitive capabilities. Organizations should develop comprehensive training programs that address both technical and operational aspects of new networking technologies. Additionally, organizations should consider partnerships with technology vendors and service providers to access specialized expertise and support.

10.3. Future research directions and emerging opportunities

The future of networking will be characterized by intelligent, automated systems that can adapt to changing demands while maintaining optimal performance and security. Organizations that proactively adopt these emerging technologies will be better positioned to support their business objectives and maintain competitive advantage in an increasingly connected world. The continuous evolution of networking technologies requires ongoing research and development to address emerging challenges and opportunities.

Several areas warrant particular attention for future research and development. The integration of AI and ML into network operations requires continued research into optimization algorithms, predictive analytics, and automated decision-making systems. The development of more sophisticated AI capabilities can enable even more autonomous and efficient network operations. Additionally, research into the security implications of AI-powered networks is essential to ensure that these systems remain secure and reliable.

The evolution of edge computing architectures presents opportunities for research into distributed processing, data management, and application architectures. The development of more efficient edge computing platforms can enable new applications and services while reducing costs and improving performance. Additionally, research into the integration of edge computing with emerging technologies such as 5G and IoT can unlock new capabilities and use cases.

The development of quantum-safe networking technologies requires continued research into post-quantum cryptography, quantum key distribution, and quantum-resistant protocols. The timeline for quantum computing development makes this research particularly urgent, as organizations must be prepared for the post-quantum era. Additionally, research into the performance implications of quantum-safe algorithms can help organizations plan for the transition to post-quantum networking.

The pursuit of sustainable networking solutions requires research into energy-efficient technologies, renewable energy integration, and circular economy principles. The development of more efficient networking technologies can reduce environmental impact while maintaining performance and reliability. Additionally, research into the lifecycle management of networking equipment can help organizations implement more sustainable practices.

Success in this evolving landscape requires a balanced approach that combines technological innovation with careful planning, skilled personnel, and ongoing investment in network infrastructure. The organizations that master this balance will be well-positioned to capitalize on the opportunities presented by these networking trends while managing the associated risks and challenges. The continuous evolution of networking technologies ensures that this field will remain dynamic and exciting, with new opportunities for innovation and improvement emerging regularly.

References

1. V. Rathore and M. Jatav, "Advancements in computer networking: A comprehensive overview of emerging technologies, protocols, and trends," *International Journal of Innovative Research in Technology and Science*, vol. 12, no. 2, pp. 416–420, Apr. 5, 2024.
2. S. Ismaeel, H. Saleemi, U. Amir, S. Ashraf, and A. Hamza, "A detailed review of latest trends, technologies applications of artificial intelligence in modern system network," *Spectrum of Engineering Sciences*, vol. 2, no. 4, pp. 198–211, Nov. 12, 2024.
3. H. Verma, N. Chauhan, and L. K. Awasthi, "A comprehensive review of 'internet of healthcare things': Networking aspects, technologies, services, applications, challenges, and security concerns," *Computer Science Review*, vol. 50, p. 100591, Nov. 1, 2023.
4. S. Nawaz, W. Salman, U. Shahid, M. L. Khokhar, M. Z. Iqbal, and A. Hamid, "A survey on latest trends and technologies of computer systems network," *Spectrum of Engineering Sciences*, vol. 2, no. 4, pp. 85–114, Nov. 14, 2024.
5. M. A. Shihab, S. A. Aswad, R. N. Othman, and S. R. Ahmed, "Advancements and challenges in networking technologies: A comprehensive survey," *in 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), IEEE*, Oct. 26, 2023, pp. 1–5.
6. L. Das, R. R. Chandan, P. Kaur, A. Singh, A. Rana, and B. D. Shivhare, "Advancements in wireless network technologies for enabling the (IoT): A comprehensive review," in *2023 6th International Conference on Contemporary Computing and Informatics (IC3I), IEEE*, vol. 6, Sep. 14, 2023, pp. 807–814.
7. Y. Harbi, Z. Aliouat, A. Refoufi, and S. Harous, "Recent security trends in internet of things: A comprehensive survey," *IEEE Access*, vol. 9, pp. 113292–113314, Aug. 9, 2021.
8. Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 1, 2021.
9. M. Moradi, M. Ahmadi, and L. PourKarimi, "Virtualized network functions resource allocation in network functions virtualization using mathematical programming," *Computer Communications*, vol. 213, pp. 100–112, 2024.
10. T. Rakkiannan, G. Ekambaram, N. Palanisamy, R. R. Ramasamy, and S. Muthusamy, "An automated network slicing at edge with software defined networking and network function virtualization: a federated learning approach," *Wireless Personal Communications*, vol. 131, pp. 1757–1775, 2023.
11. K. D. Assis, R. C. Almeida, H. Baghban, A. F. Santos, and R. Boutaba, "A two-stage reconfiguration in network function virtualization: Toward service function chain optimization," *IEEE Transactions on Network and Service Management*, May 9, 2025.
12. R. Singh, L. M. Larsen, E. O. Zaballa, M. S. Berger, C. Kloch, and L. Dittmann, "Enabling green cellular networks: A review and proposal leveraging software-defined networking, network function virtualization, and cloud-radio access network," *Future Internet*, vol. 17, no. 4, p. 161, Apr. 5, 2025.
13. M. Yang, Y. Li, D. Jin, L. Zeng, X. Wu, and A. V. Vasilakos, "Software-defined and virtualized future mobile and wireless networks: A survey," *Mobile Networks and Applications*, vol. 20, no. 1, pp. 4–18, Feb. 2015.
14. J. H. Cox, J. Chung, S. Donovan, J. Ivey, R. J. Clark, G. Riley, and H. L. Owen, "Advancing software-defined networks: A survey," *IEEE Access*, vol. 5, pp. 25487–25526, Oct. 12, 2017.
15. I. Alam, K. Sharif, F. Li, Z. Latif, M. M. Karim, B. Nour, S. Biswas, and Y. Wang, "IoT virtualization: A survey of software definition & function virtualization techniques for internet of things," *arXiv preprint arXiv:1902.10910*, Feb. 28, 2019.
16. M. Jammal, T. Singh, A. Shami, R. Asal, and Y. Li, "Software defined networking: State of the art and research challenges," *Computer Networks*, vol. 72, pp. 74–98, Oct. 29, 2014.
17. R. Cziva, S. Jouet, K. J. White, and D. P. Pezaros, "Container-based network function virtualization for software-defined networks," in *2015 IEEE Symposium on Computers and Communication (ISCC), IEEE*, Jul. 6, 2015, pp. 415–420.
18. R. Mijumbi, J. Serrat, J. L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network function virtualization: State-of-the-art and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 236–262, Sep. 4, 2015.
19. D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, Dec. 19, 2014.
20. L. Bertaux *et al.*, "Software defined networking and virtualization for broadband satellite networks," *IEEE Communications Magazine*, vol. 53, no. 3, pp. 54–60, Mar. 18, 2015.
21. M. Yang, Y. Li, D. Jin, L. Zeng, X. Wu, and A. V. Vasilakos, "Software-defined and virtualized future mobile and wireless networks: A survey," *Mobile Networks and Applications*, vol. 20, no. 1, pp. 4–18, Feb. 2015.
22. R. Sahay, W. Meng, and C. D. Jensen, "The application of software defined networking on securing computer networks: A survey," *Journal of Network and Computer Applications*, vol. 131, pp. 89–108, Apr. 1, 2019.
23. L. I. B. López, Á. L. V. Caraguay, L. J. G. Villalba, and D. López, "Trends on virtualisation with software defined networking and network function virtualisation," *IET Networks*, vol. 4, no. 5, pp. 255–263, Sep. 2015.
24. P. Goransson, C. Black, and T. Culver, "Software defined networks: A comprehensive approach". *Morgan Kaufmann*, Oct. 25, 2016.

25. Y. Li and M. Chen, "Software-defined network function virtualization: A survey," *IEEE Access*, vol. 3, pp. 2542–2553, Dec. 9, 2015.
26. A. Rahman *et al.*, "Impacts of blockchain in software-defined Internet of Things ecosystem with network function virtualization for smart applications: Present perspectives and future directions," *International Journal of Communication Systems*, vol. 38, no. 1, p. e5429, Jan. 10, 2025.
27. S. Papavassiliou, "Software defined networking (SDN) and network function virtualization (NFV)," *Future Internet*, vol. 12, no. 1, p. 7, Jan. 2, 2020.
28. Q. Duan, N. Ansari, and M. Toy, "Software-defined network virtualization: An architectural framework for integrating SDN and NFV for service provisioning in future networks," *IEEE Network*, vol. 30, no. 5, pp. 10–16, Sep. 29, 2016.
29. A. Hakiri, A. Gokhale, P. Berthou, D. C. Schmidt, and T. Gayraud, "Software-defined networking: Challenges and research opportunities for future internet," *Computer Networks*, vol. 75, pp. 453–471, Dec. 24, 2014.
30. R. Mijumbi, J. Serrat, J. L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network function virtualization: State-of-the-art and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 236–262, Sep. 4, 2015.
31. I. Alam *et al.*, "A survey of network virtualization techniques for Internet of Things using SDN and NFV," *ACM Computing Surveys (CSUR)*, vol. 53, no. 2, pp. 1–40, Apr. 16, 2020.
32. M. Yang, Y. Li, D. Jin, L. Zeng, X. Wu, and A. V. Vasilakos, "Software-defined and virtualized future mobile and wireless networks: A survey," *Mobile Networks and Applications*, vol. 20, no. 1, pp. 4–18, Feb. 2015.
33. R. Manchana, "AI-powered observability: A journey from reactive to proactive, predictive, and automated," *International Journal of Science and Research (IJSR)*, vol. 13, no. 8, pp. 1745–1755, Aug. 2024.
34. A. Al Hinai and M. Al Mazroui, "Optimizing and enhancing IT operation operating models through artificial intelligence," in *2024 2nd International Conference on Computing and Data Analytics (ICCDA), IEEE*, Nov. 12, 2024, pp. 1–5.
35. C. Kadiyala, S. Chilukoori, and S. Gangarapu, "AI-powered network automation: The next frontier in network management," *Journal of Advanced Research Engineering and Technology*, vol. 3, pp. 223–233, 2024.
36. B. Singh, "Real-time network monitoring and incident response with AI-driven automation data center and WAN transformation," Available at SSRN 5331665, Dec. 3, 2022.
37. S. Garg, "Next-gen smart city operations with AIOps & IoT: A comprehensive look at optimizing urban infrastructure," Available at SSRN 5271046, Mar. 2, 2021.
38. N. Ravichandran, A. C. Inaganti, R. Muppalaneni, and S. R. Nersu, "AI-powered workflow optimization in IT service management: Enhancing efficiency and security," *Artificial Intelligence and Machine Learning Review*, vol. 1, no. 3, pp. 10–26, Jul. 8, 2020.
39. R. R. Sukla, "The evolution of AI in software quality and cloud management: A framework for autonomous systems," *Journal of Computer Science and Technology Studies*, vol. 7, no. 6, pp. 353–359, Jun. 13, 2025.
40. A. A. Syed and E. Anazagasty, "AI-driven infrastructure automation: Leveraging AI and ML for self-healing and auto-scaling cloud environments," *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, vol. 5, no. 1, pp. 32–43, Mar. 26, 2024.
41. S. Somanathan, "AI-powered decision-making in cloud transformation: Enhancing scalability and resilience through predictive analytics," *Nanotechnology Perceptions* (ISSN: 1660-6795), vol. 20, p. S1, 2024.
42. F. Farooq, W. Ahmed, A. Akbar, F. Aslam, and R. Alyousef, "Predictive modeling for sustainable high-performance concrete from industrial wastes: A comparison and optimization of models using ensemble learners," *Journal of Cleaner Production*, vol. 292, p. 126032, Apr. 10, 2021.
43. W. Huo, W. Li, Z. Zhang, C. Sun, F. Zhou, and G. Gong, "Performance prediction of proton-exchange membrane fuel cell based on convolutional neural network and random forest feature selection," *Energy Conversion and Management*, vol. 243, p. 114367, Sep. 1, 2021.
44. W. Zhang *et al.*, "Machine learning prediction and optimization of bio-oil production from hydrothermal liquefaction of algae," *Bioresource Technology*, vol. 342, p. 126011, Dec. 1, 2021.
45. J. Guo, Y. Liu, Q. Zou, L. Ye, S. Zhu, and H. Zhang, "Study on optimization and combination strategy of multiple daily runoff prediction models coupled with physical mechanism and LSTM," *Journal of Hydrology*, vol. 624, p. 129969, Sep. 1, 2023.
46. B. Singh, "Real-time network monitoring and incident response with AI-driven automation data center and WAN transformation," Available at SSRN 5331665, Dec. 3, 2022.
47. J. K. Manda, "AI-powered threat intelligence platforms in telecom: Leveraging AI for real-time threat detection and intelligence gathering in telecom network security operations," Available at SSRN 5003638, Mar. 2, 2024.
48. Z. B. Akhtar and A. T. Rawol, "Enhancing cybersecurity through AI-powered security mechanisms," *IT journal research and development*, vol. 9, no. 1, pp. 50–67, Oct. 13, 2024.
49. G. P. Kumar *et al.*, "Art of network monitoring and security enhancement using AI-driven tools," in *Utilizing AI in Network and Mobile Security for Threat Detection and Prevention 2025*, pp. 43–58, IGI Global Scientific Publishing.
50. M. A. Farzaan, M. C. Ghanem, A. El-Hajjar, and D. N. Ratnayake, "Ai-enabled system for efficient and effective cyber incident detection and response in cloud environments," *arXiv preprint arXiv:2404.05602*, Apr. 8, 2024.
51. A. Maia *et al.*, "A survey on integrated computing, caching, and communication in the cloud-to-edge continuum," *Computer Communications*, Mar. 5, 2024.
52. D. Khalyeyev, T. Bureš, and P. Hnetynka, "Towards characterization of edge-cloud continuum," in *European Conference on Software Architecture*, Sep. 19, 2022, pp. 215–230.
53. A. Al-Dulaimy *et al.*, "The computing continuum: From IoT to the cloud," *Internet of Things*, vol. 27, p. 101272, Oct. 1, 2024.
54. N. Ali, G. Aloi, F. De Rango, C. Savaglio, and R. Gravina, "Edge-cloud continuum driven industry 4.0," *Procedia Computer Science*, vol. 253, pp. 2586–2594, Jan. 1, 2025.
55. D. Balouek-Thomert, G. Renart, A. R. Zamani, A. Simonet, and M. Parashar, "Towards a computing continuum: Enabling edge-to-cloud integration for data-driven workflows," *The International Journal of High Performance Computing Applications*, vol. 33, no. 6, pp. 1159–1174, Nov. 2019.
56. D. Rosendo, A. Costan, P. Valduriez, and G. Antoniu, "Distributed intelligence on the edge-to-cloud continuum: A systematic literature review," *Journal of Parallel and Distributed Computing*, vol. 166, pp. 71–94, Aug. 1, 2022.
57. A. Ullah *et al.*, "Micado-edge: Towards an application-level orchestrator for the cloud-to-edge computing continuum," *Journal of Grid Computing*, vol. 19, no. 4, p. 47, Dec. 2021.
58. G. Kambala, "Emergent architectures in edge computing for low-latency application," *International Journal Of Engineering And Computer Science*, vol. 13, no. 9, Sep. 2024.
59. K. Jiang, H. Zhou, X. Chen, and H. Zhang, "Mobile edge computing for ultra-reliable and low-latency communications,"

IEEE Communications Standards Magazine, vol. 5, no. 2, pp. 68–75, Apr. 23, 2021.
60. C. S. Babou *et al.*, "Home edge computing (HEC): Design of a new edge computing technology for achieving ultra-low latency," in *Edge Computing–EDGE 2018*, Jun. 25–30, 2018, pp. 3–17.
61. R. C. Thota, "Optimizing edge computing and AI for low-latency cloud workloads," *International Journal of Science and Research Archive*, vol. 13, no. 1, pp. 3484–3500, 2024.
62. R. Gupta, D. Reebadiya, and S. Tanwar, "6G-enabled edge intelligence for ultra-reliable low latency applications: Vision and mission," *Computer Standards & Interfaces*, vol. 77, p. 103521, Aug. 1, 2021.
63. M. Adhikari and A. Hazra, "6G-enabled ultra-reliable low-latency communication in edge networks," *IEEE Communications Standards Magazine*, vol. 6, no. 1, pp. 67–74, Mar. 2022.
64. A. Vladyko *et al.*, "Distributed edge computing to assist ultra-low-latency VANET applications," *Future Internet*, vol. 11, no. 6, p. 128, Jun. 4, 2019.
65. K. Aruna and G. Pradeep, "Performance and scalability improvement using IoT-based edge computing container technologies," *SN Computer Science*, vol. 1, no. 2, p. 91, Mar. 2020.
66. P. Bellavista, A. Corradi, and A. Zanni, "Integrating mobile internet of things and cloud computing towards scalability: Lessons learned from existing fog computing architectures and solutions," *International Journal of Cloud Computing*, vol. 6, no. 4, pp. 393–406, 2017.
67. A. Bali, M. Al-Osta, S. Ben Dahsen, and A. Gherbi, "Rule based auto-scalability of IoT services for efficient edge device resource utilization," *Journal of Ambient Intelligence Humanized Computing*, vol. 11, pp. 5895–5912, Dec. 2020.
68. A. Mavromatis, C. Colman-Meixner, A. P. Silva, X. Vasilakos, R. Nejabati, and D. Simeonidou, "A software-defined IoT device management framework for edge and cloud computing," *IEEE Internet Things Journal*, vol. 7, no. 3, pp. 1718–1735, Oct. 25, 2019.
69. M. Babar and M. Sohail Khan, "ScalEdge: A framework for scalable edge computing in Internet of things–based smart systems," *International Journal of Distributed Sensor Networks*, vol. 17, no. 7, p. 15501477211035332, Jul. 2021.
70. H. Kuchuk and E. Malokhvii, "Integration of IoT with cloud, fog, and edge computing: A review," *Advanced Information Systems*, vol. 8, no. 2, pp. 65–78, Jun. 4, 2024.
71. C. H. Hong and B. Varghese, "Resource management in fog/edge computing: A survey on architectures, infrastructure, and algorithms," *ACM Computing Surveys*, vol. 52, no. 5, pp. 1–37, Sep. 13, 2019.
72. J. Ren, Y. Pan, A. Goscinski, and R. A. Beyah, "Edge computing for the internet of things," *IEEE Networks*, vol. 32, no. 1, pp. 6–7, Jan. 26, 2018.
73. P. C. Jain, "Recent trends in next generation terabit Ethernet and gigabit wireless local area network," in *Proceedings International Conference on Signal Processing Communication (ICSC), IEEE*, Dec. 26, 2016, pp. 106–110.
74. A. S. George, A. H. George, T. Baskar, and D. Pandey, "The transformation of the workspace using multigigabit ethernet," *Partners Universal International Research Journal*, vol. 1, no. 3, pp. 34–43, Sep. 29, 2022.
75. D. J. Law, W. W. Diab, A. Healey, S. B. Carlson, and V. Maguire, "IEEE 802.3 industry connections Ethernet bandwidth assessment," *IEEE 802.3 BWA Ad Hoc Rep.*, Jul. 19, 2012.
76. A. Zapata *et al.*, "Next-generation 100-gigabit metro ethernet (100 GbME) using multiwavelength optical rings," *Journal of Lightwave Technology*, vol. 22, no. 11, pp. 2420–2426, Nov. 1, 2004.
77. P. Vetter, "The future of broadband access," in *The Future X Network*, CRC Press, Sep. 3, 2018, pp. 227–254.
78. J. Zou, "Optical access technologies for next-gen mobile applications," in *Handbook of Radio and Optical Networks Convergence*, Singapore: Springer Nature Singapore, Oct. 2, 2024, pp. 259–276.
79. C. F. Lam, "Beyond gigabit: Application and development of high-speed ethernet technology," in *Optical Fiber Telecommun. IV-B*, Academic Press, Jan. 1, 2002, pp. 514–563.
80. J. Su *et al.*, "Technology trends in large-scale high-efficiency network computing," *Frontiers of Information Technology Electronic Engineering*, vol. 23, no. 12, pp. 1733–1746, Dec. 2022.
81. Y. Benkler *et al.*, "Next generation connectivity: A review of broadband internet transitions and policy from around the world,"
82. A. Wallibai and G. R. Deshpande, "Automotive ethernet: High-speed in-vehicle networking for next-generation electronics," *World Journal of Advanced Research and Reviews*, vol. 8, no. 2, pp. 353–368, 2020.
83. S. Vitturi, C. Zunino, and T. Sauter, "Industrial communication systems and their future challenges: Next-generation Ethernet, IIoT, and 5G," *Proceedings of IEEE*, vol. 107, no. 6, pp. 944–961, May 15, 2019.
84. D. C. Dowden, R. D. Gitlin, and R. L. Martin, "Next-generation networks," *Bell Labs Technical Journal*, vol. 3, no. 4, pp. 3–14, Oct. 1998.
85. A. S. George, A. H. George, T. Baskar, and D. Pandey, "The transformation of the workspace using multigigabit ethernet," *Partners Universal International Research Journal*, vol. 1, no. 3, pp. 34–43, Sep. 29, 2022.
86. T. M. Egyedi and M. H. Sherif, "Standards' dynamics through an innovation lens: Next generation ethernet networks," in *Proceedings First ITU-T Kaleidoscope Academic Conference-Innovations NGN: Future Network and Services, IEEE*, May 12, 2008, pp. 127–134.
87. R. Rajabiun and C. Middleton, "Strategic choice and broadband divergence in the transition to next generation networks: Evidence from Canada and the US," *Telecommunications Policy*, vol. 42, no. 1, pp. 37–50, Feb. 1, 2018.
88. A. Gumaste and S. Akhtar, "Evolution of packet-optical integration in backbone and metropolitan high-speed networks: A standards perspective," *IEEE Communications Magazine*, vol. 51, no. 11, pp. 105–111, Nov. 11, 2013.
89. A. Wallibai and G. R. Deshpande, "Automotive ethernet: High-speed in-vehicle networking for next-generation electronics," *World Journal of Advanced Research and Reviews*, vol. 8, no. 2, pp. 353–368, 2020.
90. S. Vitturi, C. Zunino, and T. Sauter, "Industrial communication systems and their future challenges: Next-generation Ethernet, IIoT, and 5G," *Proceedings of IEEE*, vol. 107, no. 6, pp. 944–961, May 15, 2019.
91. C. A. Thekkath and H. M. Levy, "Limits to low-latency communication on high-speed networks," *ACM Transactions on Computer Systems*, vol. 11, no. 2, pp. 179–203, May 1, 1993.
92. J. Zou *et al.*, "Advanced optical access technologies for next-generation (5G) mobile networks," *Journal of Optical Communications and Networking*, vol. 12, no. 10, pp. D86–D98, Oct. 1, 2020.
93. N. J. Gomes *et al.*, "Boosting 5G through ethernet: How evolved fronthaul can take next-generation mobile to the

next level," *IEEE Vehicular Technology Magazine*, vol. 13, no. 1, pp. 74–84, Feb. 1, 2018.
94. S. Pandiaraj *et al.*, "Optimization of IoT circuit for flexible optical network system with high speed utilization," *Optical and Quantum Electronics*, vol. 55, no. 13, p. 1206, Dec. 2023.
95. S. Kamil, L. Oliker, A. Pinar, and J. Shalf, "Communication requirements and interconnect optimization for high-end scientific applications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 2, pp. 188–202, Apr. 17, 2009.
96. L. Xue *et al.*, "Towards fair and low latency next generation high speed networks: AFCD queuing," *Journal of Network and Computer Applications*, vol. 70, pp. 183–193, Jul. 1, 2016.
97. V. Stafford, "Zero trust architecture," *NIST Special Publication*, vol. 800, no. 207, pp. 800–207, Aug. 2020.
98. Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on zero trust architecture: Challenges and future trends," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 6476274, 2022.
99. M. J. Khan, "Zero trust architecture: Redefining network security paradigms in the digital age," *World Journal of Advanced Research and Reviews*, vol. 19, no. 3, pp. 105–116, 2023.
100. S. Sarkar *et al.*, "Security of zero trust networks in cloud computing: A comparative review," *Sustainability*, vol. 14, no. 18, p. 11213, Sep. 7, 2022.
101. P. Assunção, "A zero trust approach to network security," in *Proceedings Digital Privacy and Security Conference* , Porto, Portugal, vol. 2019, Jan. 16, 2019.
102. O. C. Edo *et al.*, "Zero trust architecture: Trend and impact on information security," *International Journal Emerging Technology and Advanced Engineering*, vol. 12, no. 7, pp. 140–147, 2022.
103. P. Dhiman *et al.*, "A review and comparative analysis of relevant approaches of zero trust network model," *Sensors*, vol. 24, no. 4, p. 1328, Feb. 19, 2024.
104. J. Kindervag, "Build security into your network's DNA: The zero trust network architecture," *Forrester Research Inc.*, vol. 27, pp. 1–6, Nov. 5, 2010.
105. X. Yan and H. Wang, "Survey on zero-trust network security," in *International Conference on Artificial Intelligence and Security*, Singapore: Springer Singapore, Jul. 17, 2020, pp. 50–60.
106. W. R. Simpson and K. E. Foltz, "Network segmentation and zero trust architectures," in *Lecture Notes in Engineering and Computer Science, Proceedings of the World Congress on Engineering (WCE)*, 2021, pp. 201–206.
107. C. Ravi *et al.*, "Beyond the firewall: Implementing zero trust with network microsegmentation," *Nanotechnology Perceptions*, vol. 21, pp. 560–578, 2025.
108. L. Xie *et al.*, "A micro-segmentation protection scheme based on zero trust architecture," in *ISCTT 2021; 6th International Conference on Information Science, Computer Technology and Transportation*, Nov. 26, 2021, pp. 1–4.
109. S. Keeriyattil, "Microsegmentation and zero trust: Introduction," in *Zero Trust Networks with VMware NSX: Build Highly Secure Network Architectures for Your Data Centers*, Berkeley, CA: Apress, Dec. 1, 2019, pp. 17–31.
110. N. Basta, M. Ikram, M. A. Kaafar, and A. Walker, "Towards a zero-trust micro-segmentation network security strategy: an evaluation framework," in *NOMS 2022 - IEEE/IFIP Network Operations and Management Symposium*, Apr. 25, 2022, pp. 1–7.
111. N. F. Syed *et al.*, "Zero trust architecture (ZTA): A comprehensive survey," *IEEE Access*, vol. 10, pp. 57143–57179, May 12, 2022.
112. S. Ahmadi, "Zero trust architecture in cloud networks: Application, challenges and future opportunities," *Journal of Engineering Research and Reports*, vol. 26, no. 2, pp. 215–228, Feb. 13, 2024.
113. S. Tiwari, W. Sarma, and A. Srivastava, "Integrating artificial intelligence with zero trust architecture: enhancing adaptive security in modern cyber threat landscape," *International Journal of Research And Analytical Reviews*, vol. 9, pp. 712–728, 2022.
114. P. John, S. S. Nittala, and S. Chandanapalli, "Collating threat intelligence for zero trust future using open-source tools," in *Implementing Enterprise Cybersecurity with Opensource Software and Standard Architecture*, River Publishers, Sep. 2022, pp. 111–132.
115. B. T. Ofili, E. O. Erhabor, and O. T. Obasuyi, "Enhancing federal cloud security with AI: Zero trust, threat intelligence, and CISA compliance," *World Journal of Advanced Research and Review*, 2025.
116. N. F. Syed *et al.*, "Zero trust architecture (ZTA): A comprehensive survey," *IEEE Access*, vol. 10, pp. 57143–57179, May 2022.
117. M. J. Khan, "Zero trust architecture: Redefining network security paradigms in the digital age," *World Journal of Advanced Research and Reviews*, vol. 19, no. 3, pp. 105–116, 2023.
118. H. Joshi, "Emerging technologies driving zero trust maturity across industries," *IEEE Open Journal of the Computer Society*, Nov. 22, 2024.
119. S. Arora and A. Tewari, "Zero trust architecture in IAM with AI integration," *Int. J. Sci. Res. Arch.*, vol. 8, no. 2, pp. 737–745, Apr. 2023.
120. J. K. Manda, "Zero trust architecture in telecom: Implementing zero trust architecture principles to enhance network security and mitigate insider threats in telecom operations," *Journal of Innovative Technologies*, vol. 5, no. 1, Nov. 15, 2022.
121. D. Minoli, "Designing green networks with reduced carbon footprints," *Journal of Telecommunications Management*, vol. 3, no. 1, Apr. 1, 2010.
122. J. Lorincz, A. Capone, and J. Wu, "Greener, energy-efficient and sustainable networks: State-of-the-art and new trends," *Sensors*, vol. 19, no. 22, p. 4864, Nov. 8, 2019.
123. J. Light, "Green networking: a simulation of energy efficient methods," *Procedia Computer Science*, vol. 171, pp. 1489–1497, Jan. 1, 2020.
124. S. S. Sandhu, A. Rawal, P. Kaur, and N. Gupta, "Major components associated with green networking in information communication technology systems," in *2012 International Conference on Computing, Communication and Applications*, Feb. 22, 2012, pp. 1–6.
125. S. Zeadally, S. U. Khan, and N. Chilamkurti, "Energy-efficient networking: Past, present, and future," *The Journal of Supercomputing*, vol. 62, pp. 1093–1118, Dec. 2012.
126. W. Y. Leong, Y. Z. Leong, and W. S. Leong, "Green communication systems: Towards sustainable networking," in *2024 5th International Conference on Information Science, Parallel and Distributed Systems (ISPDS), IEEE*, May 31, 2024, pp. 559–564.
127. M. Uddin and A. A. Rahman, "Energy efficiency and low carbon enabler green IT framework for data centers considering green metrics," *Renewable and Sustainable Energy Reviews*, vol. 16, no. 6, pp. 4078–4094, Aug. 1, 2012.
128. R. Bolla *et al.*, "The potential impact of green technologies in next-generation wireline networks: Is there room for energy

saving optimization?," *IEEE Communications Magazine*, vol. 49, no. 8, pp. 80–86, Aug. 11, 2011.
129. A. Israr, Q. Yang, W. Li, and A. Y. Zomaya, "Renewable energy powered sustainable 5G network infrastructure: Opportunities, challenges and perspectives," *Journal of Network and Computer Applications*, vol. 175, p. 102910, Feb. 1, 2021.
130. S. B. Sarte, Sustainable infrastructure: the guide to green engineering and design, John Wiley & Sons, Sep. 7, 2010.
131. M. Piechowski and A. Weerakkody, "Integrated renewable energy infrastructure-challenges and opportunities," *Energy*, pp. 52–57, 2011.
132. M. Bagheri, N. Shirzadi, E. Bazdar, and C. A. Kennedy, "Optimal planning of hybrid renewable energy infrastructure for urban sustainability: Green Vancouver," *Renewable and Sustainable Energy Reviews*, vol. 95, pp. 254–264, Nov. 1, 2018.
133. D. S. Olaleye *et al.*, "Advancing green communications: the role of radio frequency engineering in sustainable infrastructure design," *International Journal of Latest Technology in Engineering, Management & Applied Science (IJLTEMAS)*, vol. 13, no. 5, pp. 113, 2024.
134. S. M. Khoshnava *et al.*, "Green efforts to link the economy and infrastructure strategies in the context of sustainable development," *Energy*, vol. 193, p. 116759, Feb. 15, 2020.
135. O. A. Oluokun *et al.*, "Integrating renewable energy solutions in urban infrastructure: A policy framework for sustainable development,"
136. B. R. Dawadi, D. B. Rawat, S. R. Joshi, and M. M. Keitsch, "Towards energy efficiency and green network infrastructure deployment in Nepal using software defined IPv6 network paradigm," *The Electronic Journal of Information Systems in Developing Countries*, vol. 86, no. 1, p. e12114, Jan. 2020.
137. J. Li *et al.*, "Green environment and circular economy: A state-of-the-art analysis," *Sustainable Energy Technologies and Assessments*, vol. 52, p. 102106, Aug. 1, 2022.
138. T. L. Chen *et al.*, "Implementation of green chemistry principles in circular economy system towards sustainable development goals: Challenges and perspectives," *Science of the Total Environment*, vol. 716, p. 136998, May 10, 2020.
139. D. Romero and A. Molina, "Green virtual enterprise breeding environments: A sustainable industrial development model for a circular economy," in *Collaborative Networks in the Internet of Services*. Berlin Heidelberg: Springer, 2012, pp. 427–436.
140. G. Hatzivasilis *et al.*, "The green blockchains of circular economy," *Electronics*, vol. 10, no. 16, p. 2008, Aug. 19, 2021.
141. M. Niero and X. C. Rivera, "The role of life cycle sustainability assessment in the implementation of circular economy principles in organizations," *Procedia CIRP*, vol. 69, pp. 793–798, Jan. 1, 2018.
142. V. Kandpal *et al.*, "Circular economy principles: Shifting towards sustainable prosperity," in *Sustainable energy transition: Circular economy and sustainable financing for environmental, social and governance (ESG) practices*, Springer Nature Switzerland, Feb. 8, 2024, pp. 125–165.
143. B. Suárez-Eiroa *et al.*, "Operational principles of circular economy for sustainable development: Linking theory and practice," *Journal of Cleaner Production*, vol. 214, pp. 952–963, Mar. 20, 2019.
144. O. Rodríguez-Espíndola *et al.*, "The role of circular economy principles and sustainable-oriented innovation to enhance social, economic and environmental performance: Evidence from Mexican SMEs," *International Journal of Production Economics*, vol. 248, p. 108495, Jun. 1, 2022.
145. J. Alonso, L. Orue-Echevarria, V. Casola, A. I. Torre, M. Huarte, E. Osaba, and J. L. Lobo, "Understanding the challenges and novel architectural models of multi-cloud native applications–a systematic literature review," *Journal of Cloud Computing*, vol. 12, no. 1, p. 6, Jan. 2023.
146. S. R. Gundu, C. A. Panem, and A. Thimmapuram, "Hybrid IT and multi cloud an emerging trend and improved performance in cloud computing," *SN Computer Science*, vol. 1, no. 5, p. 256, Sep. 2020.
147. S. Natarajan and J. Jacob, Multi-Cloud Handbook for Developers: Learn how to design and manage cloud-native applications in AWS, Azure, GCP, and more. Packt Publishing Ltd, Feb. 29, 2024.
148. V. Baladari, "Enhancing performance and security in multi-cloud and hybrid-cloud environments," *International Journal of Core Engineering and Management*, vol. 7, no. 11, pp. 53–265, 2024.
149. N. H. Anh, "Hybrid cloud migration strategies: Balancing flexibility, security, and cost in a multi-cloud environment," *Transactions on Machine Learning, Artificial Intelligence, and Advanced Intelligent Systems*, vol. 14, no. 10, pp. 14–26, Oct. 7, 2024.
150. V. K. Munnangi, "Multi-cloud and hybrid cloud strategies for enterprise API architectures," *Journal of Computer Science and Technology Studies*, vol. 7, no. 4, pp. 79–90, May 10, 2025.
151. S. Gupta, "Hybrid cloud integration and multicloud deployments a comprehensive review of strategies, challenges, and best practices," *International Journal of Advanced Research in Computer Science*, vol. 16, no. 2, Mar. 1, 2025.
152. S. Hirai, T. Tojo, S. Seto, and S. Yasukawa, "Automated provisioning of cloud-native network functions in multi-cloud environments," in *2020 6th IEEE Conference on Network Softwarization (NetSoft), IEEE*, Jun. 29, 2020, pp. 1–3.
153. L. Osmani, T. Kauppinen, M. Komu, and S. Tarkoma, "Multi-cloud connectivity for kubernetes in 5G networks," *IEEE Communications Magazine*, vol. 59, no. 10, pp. 42–47, Nov. 26, 2021.
154. S. R. Gundu, C. A. Panem, and A. Thimmapuram, "Hybrid IT and multi cloud an emerging trend and improved performance in cloud computing," *SN Computer Science*, vol. 1, no. 5, p. 256, Sep. 2020.
155. K. J. Merseedi and S. R. Zeebaree, "The cloud architectures for distributed multi-cloud computing: A review of hybrid and federated cloud environment," *The Indonesian Journal of Computer Science*, vol. 13, no. 2, Apr. 1, 2024.
156. S. R. Julakanti, N. S. Sattiraju, and R. Julakanti, "Multi-cloud security: Strategies for managing hybrid environments," *NeuroQuantology*, vol. 20, no. 11, pp. 10063–10074, 2022.
157. N. H. Anh, "Hybrid cloud migration strategies: Balancing flexibility, security, and cost in a multi-cloud environment," *Transactions on Machine Learning, Artificial Intelligence, and Advanced Intelligent Systems*, vol. 14, no. 10, pp. 14–26, Oct. 7, 2024.
158. B. Desai and K. Patil, "Demystifying the complexity of multi-cloud networking," *Asian American Research Letters Journal*, vol. 1, no. 4, Jun. 19, 2024.
159. K. J. Merseedi and S. R. Zeebaree, "The cloud architectures for distributed multi-cloud computing: a review of hybrid and federated cloud environment," *The Indonesian Journal of Computer Science*, vol. 13, no. 2, Apr. 1, 2024.
160. B. Desai and K. Patil, "Demystifying the complexity of multi-cloud networking," *Asian American Research Letters Journal*, vol. 1, no. 4, Jun. 19, 2024.

161. B. Yeganeh, R. Durairajan, R. Rejaie, and W. Willinger, "A first comparative characterization of multi-cloud connectivity in today's internet," in *International Conference on Passive and Active Network Measurement*, Cham: Springer International Publishing, Mar. 18, 2020, pp. 193–210.
162. M. Alaluna, E. Vial, N. Neves, and F. M. Ramos, "Secure multi-cloud network virtualization," *Computer Networks*, vol. 161, pp. 45–60, Oct. 9, 2019.
163. J. George, "Optimizing hybrid and multi-cloud architectures for real-time data streaming and analytics: Strategies for scalability and integration," *World Journal of Advanced Engineering Technology and Sciences*, vol. 7, no. 1, pp. 10–30574, Oct. 29, 2022.
164. G. H. Carvalho, I. Woungang, A. Anpalagan, M. Jaseemuddin, and E. Hossain, "Intercloud and HetNet for mobile cloud computing in 5G systems: Design issues, challenges, and optimization," *IEEE Network*, vol. 31, no. 3, pp. 80–89, May 26, 2017.
165. B. Kumar, "Challenges and solutions for integrating AI with Multi-cloud architectures," *International Journal of Multidisciplinary Innovation and Research Methodology*, pp. 2960–068, Dec. 2022.
166. M. Angamuthu, "Optimizing multi-cloud business intelligence: A framework for balancing cost, performance, and security," *Journal of Computer Science and Technology Studies*, vol. 7, no. 4, pp. 427–437, May 15, 2025.
167. F. Samad, A. Abbasi, Z. A. Memon, A. Aziz, and A. Rahman, "The future of internet: IPv6 fulfilling the routing needs in internet of things," *International Journal of Future Generation Communication and Networking*, vol. 11, no. 1, pp. 13–22, Jan. 1, 2018.
168. S. Gupta, R. Verma, and N. Dhanda, "Introduction to Next-Generation Internet and Distributed Systems," *Decentralized Systems and Distributed Computing*, pp. 1–34, Jul. 31, 2024.
169. A. Hamarsheh, "Assessing the progress of transition to IPv6: A global perspective," *IETE Journal of Research*, pp. 1–5, Apr. 17, 2025.
170. Y. Chai, X. J. Zeng, and Z. Liu, "The future of wireless mesh network in next-generation communication: A perspective overview," *Evolving Systems*, vol. 15, no. 4, pp. 1635–1648, Aug. 2024.
171. K. Igulu, F. Onuodu, and T. P. Singh, "IPV6: Strengths and limitations," in *Communication Technologies and Security Challenges in IoT: Present and Future*, Singapore: Springer Nature Singapore, Mar. 26, 2024, pp. 147–172.
172. E. Blancaflor, C. D. Unciano, E. M. Arcigal, I. J. Contreras, and M. Abisado, "Towards the increasing usage of IPv6 & its implication: A literature review," in *Proceedings of the 2024 10th International Conference on Computing and Artificial Intelligence*, Apr. 26, 2024, pp. 373–378.
173. J. Yedalla, "Quantum-safe cryptography: Navigating the future of cybersecurity in the post-quantum era," *International Journal of Science and Research (IJSR)*, vol. 14, no. 2, pp. 249–253, 2025.
174. M. A. Khan, S. Javaid, S. A. Mohsan, M. Tanveer, and I. Ullah, "Future-proofing security for UAVs with post-quantum cryptography: A review," *IEEE Open Journal of the Communications Society*, Oct. 28, 2024.
175. A. Aydeger, E. Zeydan, A. K. Yadav, K. T. Hemachandra, and M. Liyanage, "Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography," in *2024 15th International Conference on Network of the Future (NoF), IEEE*, Oct. 2, 2024, pp. 195–203.
176. M. Imran, A. B. Altamimi, W. Khan, S. Hussain, and M. Alsaffar, "Quantum cryptography for future networks security: A systematic review," *IEEE Access*, Nov. 22, 2024.
177. P. C. Nwaga and S. Nwagwughiagwu, "Exploring the significance of quantum cryptography in future network security protocols," *World J Adv Res Reviews*, vol. 24, no. 3, pp. 817–833, 2024.
178. Y. Baseri, V. Chouhan, and A. Hafid, "Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols," *Computers & Security*, p. 103883, May 1, 2024.
179. H. Fang, P. Yu, C. Tan, J. Zhang, D. Lin, L. Zhang, Y. Zhang, W. Li, and L. Meng, "Self-healing in knowledge-driven autonomous networks: Context, challenges, and future directions," *IEEE Network*, Jun. 19, 2024.
180. J. Feng, T. Yu, K. Zhang, and L. Cheng, "Integration of multi-agent systems and artificial intelligence in self-healing subway power supply systems: Advancements in fault diagnosis, isolation, and recovery," *Processes*, vol. 13, no. 4, p. 1144, Apr. 10, 2025.
181. S. R. Rouholamini, M. Mirabi, R. Farazkish, and A. Sahafi, "Proactive self-healing techniques for cloud computing: A systematic review," *Concurrency and Computation: Practice and Experience*, vol. 36, no. 24, p. e8246, Nov. 1, 2024.
182. S. Harsha and F. Sreeharsha, "'Data privacy and security considerations in self-healing networks: Balancing automation and confidentiality," *Int. Res. J. Eng. Technol. (IRJET)*, vol. 11, no. 5, pp. 1–1, May 2024.
183. W. Dang, R. Huang, Y. Yu, and Y. Zhang, Autonomous Driving Network: Network Architecture in the Era of Autonomy. CRC Press, Jan. 15, 2024.
184. P. Phogat, S. Sharma, S. Rai, and J. Thakur, "Future Directions and Opportunities," in *Self-healing Materials 2025*, Singapore: Springer, 2025, pp. 309–338.