future internet

MDPI

Review

Enterprise Networking Optimization: A Review of Challenges, Solutions, and Technological Interventions

Oladele Afolalu * and Mohohlo Samuel Tsoeu

Department of Electronic and Computer Engineering, Durban University of Technology,
Durban 4001, South Africa; mohohlot@dut.ac.za
* Correspondence: oladelea@dut.ac.za

Abstract: Enterprise networking optimization has become crucial recently due to increasing demand for a secure, adaptable, reliable, and interoperable network infrastructure. Novel techniques to optimize network security and toimprove scalability and efficiency are constantly being developed by network enablers, particularly in more challenging multi-cloud and edge scenarios. This paper, therefore, presents a comprehensive review of the traditional and most recent developments in enterprise networking. We structure the paper with particular emphasis on the adoption of state of-the-art technologies, such as software-defined wide area network(SD-WAN), secure access service edge (SASE) architecture, and network automation, driven by artificial intelligence (AI). The review also identifies various challenges associated with the adoption of the aforementioned technologies. These include operational complexity, cybersecurity threats, and trade-offs between cost-effectiveness and high performance requirements. Furthermore, the paper examines how different organizations are addressing a plethora of challenges by exploiting these technological innovations to drive robust and agile business interconnectivity. The review is concluded with an outline of possible solutions and future prospects, capable of promoting digital transformation and enhancing seamless connectivity within the enterprise networking environment.

Keywords: cybersecurity; cloud computing; edge computing; enterprise networking; SD-WAN

check for updates

Academic Editor: Paolo Bellavista

Received: 29 January 2025
Revised: 12 March 2025
Accepted: 17 March 2025
Published: 21 March 2025

Citation: Afolalu, O.; Tsoeu, M.S. Enterprise Networking Optimization: A Review of Challenges, Solutions, and Technological Interventions. *Future Internet* **2025**, *17*, 133. https://doi.org/10.3390/fi17040133

1. Introduction

Innovations in cloud computing, edge computing, artificial intelligence, and improved cybersecurity have fundamentally changed the enterprise networking landscape in the modern era [1–3]. Today, enterprise networks are the foundation of digital transformation. They provide scalability, speed, and flexibility needed to meet the needs of contemporary business environments. Some of these are increased data throughput, hybrid and remote work environments, and easy access to varied applications in the cloud [4–6]. In order to satisfy these requirements, significant advancements in zero trust network access (ZTNA), software-defined networking (SDN), and enhanced network automation have become essential [7,8]. These interventions enable enterprises to lower costs, enhance security features, and optimize organizational activities. An enterprise network represents an organization's local internet that allows file sharing, system access, and communication between employees and devices [9–11]. Through effective communication, users can analyze the performance of the connecting environment that propels business operations. Businesses, organizations, devices, and applications should maintain constant communication to facilitate messaging, calls, emails, and all forms of office operations. Such communication can exist between the staff, spreading across various local and international branches [12,13]. Generally, an enterprise network consists of hardware and software units, including different structures that facilitate end-to-end service delivery [14]. A well-managed network supports thousands of devices and allows many users to work reliably in hundreds of sites worldwide at any time. The structure of these networks relies on intranets and extranets, intrinsically built on both local area network (LAN) and wide area network (WAN) technologies [15]. Security issues on the networks are then addressed through efficient management of internal and external traffic flow patterns [16,17].

Enterprise networks utilize advanced networking and security technologies that allow users and devices to communicate securely and remotely from the office [18]. To perform optimally, there is need to incorporate high-speed and reliable information technology (IT) infrastructure. This helps to reduce communication protocols, alleviate bottlenecks, optimize uptime, and enable smooth operations [19,20]. In addition, hundreds of networking devices, such as switches and routers, are deployed to interconnect servers and end-user workstations. The interconnection can either be through wired (copper), fiber-optic, or wireless technologies [21]. Hence, seamless communication and device interoperability can be facilitated across a wide range of devices, such as smartphones, computers, tablets, and printers, with different operating systems (Android, Apple, Linux, and Windows). To provide guaranteed security, network connectivity in geographically heterogeneous locations is encrypted using virtual private networks (VPNs) [22]. The purpose of VPN encryption in enterprise environments is to restrict connectivity to specific users, devices, and facilities, unlike the internet.

Apart from a connection provided to a user via a single router, an enterprise network hosts a series of connectivity between different devices and the internet. In large networks, an autonomous system number (ASN) may be assigned to provide seamless connection [23]. The earlier method employed in enterprise networking was to connect users and devices to centralized data centers located within the same premises. These data centers served as data repositories and platforms for running applications. In this manner, users and devices were granted access to the head office via LAN [24–26]. Thus, the LAN in each office usually formed a connected link to other offices through a large enterprise WAN. This was usually implemented via dedicated multiprotocol label switching (MPLS) links [27–30], as shown in Figure 1.

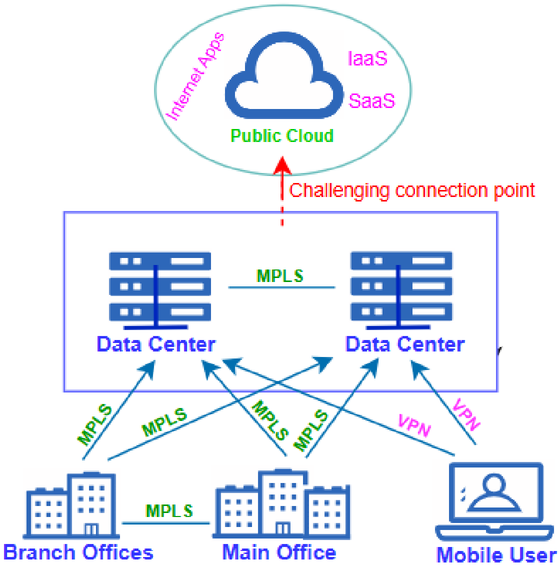

Figure 1. Interconnectivity in enterprise network using MLPS.

However, the current reality of network demands in terms of security has rendered traditional network connectivity unsuitable for the fast-paced needs of modern organizations. Many applications described earlier are currently being combined as a form of cloud migration to address the new security challenges of businesses and organizations [30,31]. Therefore, this paper seeks to provide a comprehensive survey of various state-of-the-art technologies that have contributed to the evolutionary trends in enterprise networking. To the best of our knowledge, there is no existing literature that provides a detailed review of enterprise network evolution in the context of challenges, solutions, and new trends as presented in this paper. Furthermore, it is essential to present an updated overview of enterprise networking, considering its importance in supporting businesses to run highly secure and reliable networking systems.

Our specific contributions in this paper are summarized as follows:

1. Summary of traditional and state-of-the-art enterprise networking technologies and the impact on organizational transformation.
2. Discussion of the challenges and opportunities of enterprise networks, with special focus on security challenges and their limitations towards achieving seamless and reliable network connectivity.
3. Presentation of new trends and potential future research directions in the deployment of enterprise networks for next-generation business solutions.

The rest of the paper is organized as follows. Section 2 introduces the main composition of enterprise networking architecture, which consists of access, distribution, and core layers, in addition to the corresponding sub-structures. Section 3 presents the benefits of an optimized enterprise networking system to herald the significance of functionalities discussed in the subsequent sections. Section 4 discusses various network and security protocols that are aggregated to support proper functioning of enterprise networks. Major state-of-the-art technological innovations in enterprise networking are discussed as new trends and focus for future research directions in Section 5. Finally, the paper is concluded in Section 6. An overview of the organization and structure of the paper is shown in Figure 2.

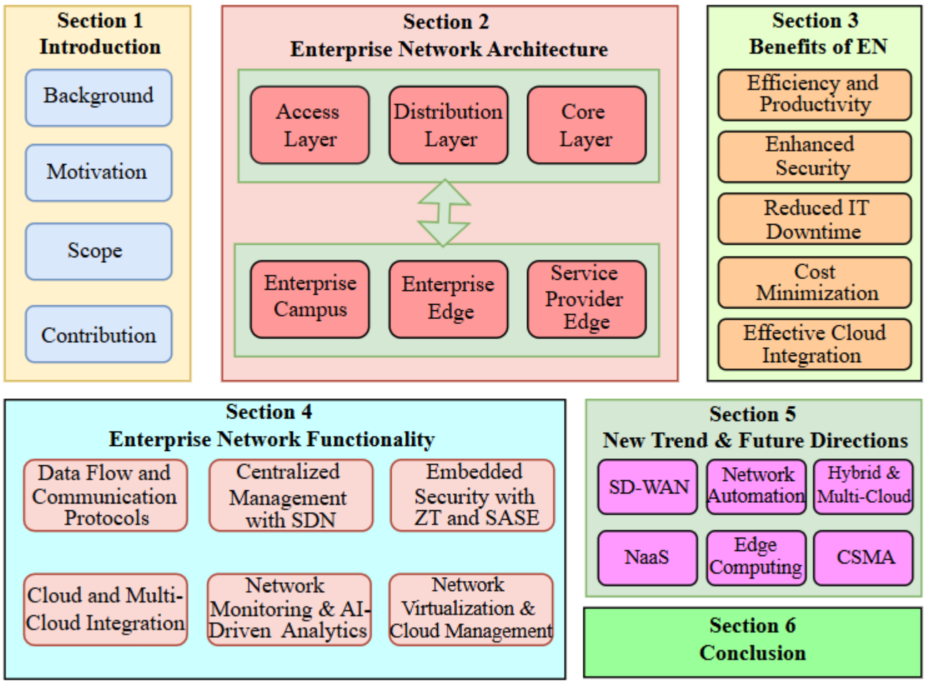
Section 1
Introduction
Background
Motivation
Scope
Contribution
Section 2
Enterprise Network Architecture
Access Layer
Distribution Layer
Core Layer
Enterprise Campus
Enterprise Edge
Service Provider Edge
Section 3
Benefits of EN
Efficiency and Productivity
Enhanced Security
Reduced IT Downtime
Cost Minimization
Effective Cloud Integration
Section 4
Enterprise Network Functionality
Data Flow and Communication Protocols
Centralized Management with SDN
Embedded Security with ZT and SASE
Cloud and Multi-Cloud Integration
Network Monitoring & AI-Driven Analytics
Network Virtualization & Cloud Management
Section 5
New Trend & Future Directions
SD-WAN
Network Automation
Hybrid & Multi-Cloud
NaaS
Edge Computing
CSMA
Section 6
Conclusion

Figure 2. Organization and Structure of the paper.

2. Enterprise Networking Architecture

Within an organization, data, applications and communication protocols interact through the underlying layout of the enterprise network structure and architecture. Enterprise networks were initially planned as centralized, hierarchical, on-premises data centers [32,33]. This model has developed into recent architectures which have since evolved to accommodate distributed and cloud-based systems [34–36]. An enterprise network is structured and designed to serve as bedrock for effective resource management, data interchange, and security in a corporate setting. Enterprise networks are organized around essential elements and frameworks that facilitate local and remote connectivity, promoting smooth operations in multi-cloud and hybrid configurations [37–40]. Nowadays, the multi-tiered architecture is a popular structure in enterprise networking [41]. It divides the network into three distinct layers: access, distribution, and core [42]. This provides improved security and allows free flow of traffic by leveraging the capability of software-defined networking (SDN) technologies. The SDN framework separates the control plane from the data plane, so that the network can be managed efficiently [43,44]. An overview of the common architectural components in enterprise networking is discussed in the following, with Figure 3 showing a typical structure.

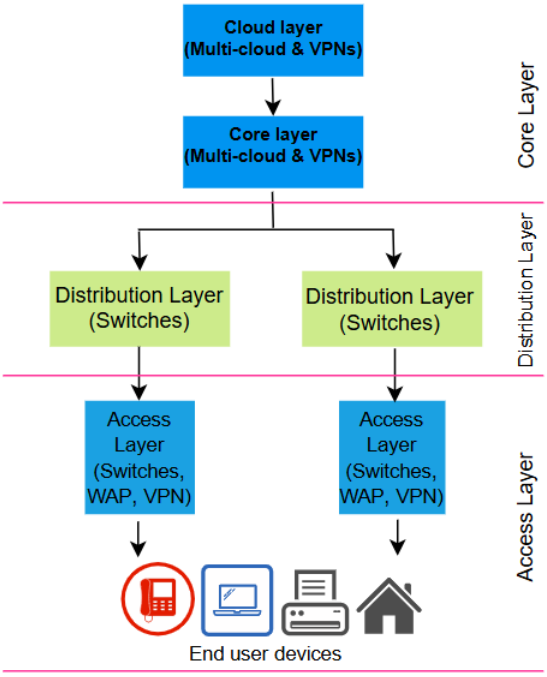

Figure 3. Major architectural components in enterprise network.

2.1. Access Layer

This layer provides connectivity to end users through the routers, switches and wireless access points. It is the closest layer to the end users. The access layer relies entirely on network segmentation and access controls as two security features frequently deployed to protect the network periphery [45]. At this point, the access layer connects to the distribution layer.

2.2. Distribution Layer

The distribution layer is an intermediary layer where data aggregation takes place from access to core layer. Hence, it can also be referred to alternatively as the aggregation layer. Switches and routing features are usually incorporated for policy governance, traffic management, security measure implementation, and quality of service provisioning [45].

2.3. Core Layer

The core layer can be regarded as the network backbone which connects several cascaded layers of the network. Fault isolation is typically carried out in the core layer. It is also noteworthy that the core can function as a rented leased line provided by an internet service provider (ISP) to large organizations in order to reduce costs [46]. Any little downtime can impact the network and therefore result in massive loss of revenue. Thus, the core layer is expected to provide high levels of reliability, redundancy, and reduced latency.

Distribution of the network into these three-layered hierarchical structures greatly helps to manage and organize the network efficiently. While the aforementioned structure is maintained, there exists further classification of the network into enterprise campus, enterprise edge and Service Provider Edge. The sub-division is altogether termed eEnterprise composite network model (ECNM) [46], as depicted in Figure 4. The ECNM network sub-structure is very important due to its advantage in offering logical, physical, and hierarchical functional design.

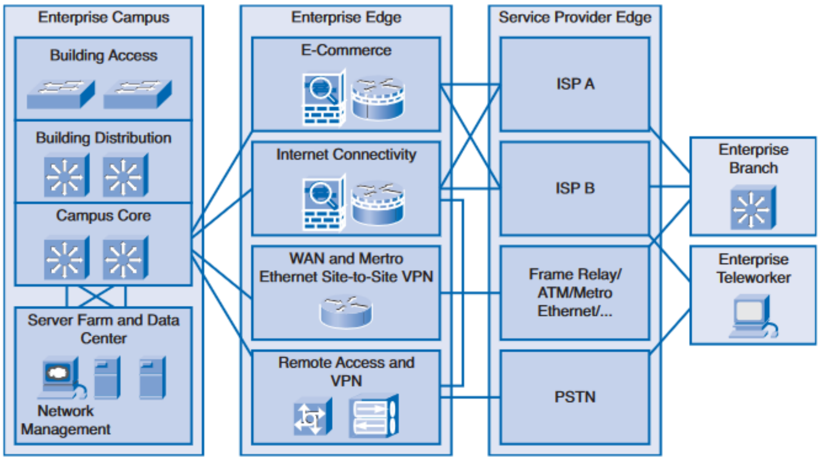

Figure 4. Classification of enterprise composite network model [46].

2.4. The Enterprise Campus

The enterprise sub-classification is a campus infrastructure that encompasses the network management facility and server farm or server cluster. Both layer 2 and layer 3 switches are used to provide appropriate network connectivity in the building access branch [47]. Thus, the adjoining building distribution compartment, which uses layer 3 devices, is connected via the trunk and virtual LAN (VLAN) links to the building access traffic aggregation. Therefore, implementation of access control, quality of service (QoS), and routing are all executed by this module.

The campus core segment ensures ultra-fast and high speed connectivity between the three blocks [48], i.e., the building distribution section, data center farms, and the enterprise edge. It also reduces unnecessary redundancy in the devices and links. Hence, the goal of achieving adequate fault tolerance and fast convergence will be met by this segment. The function of network management is to ensure enhanced network performance for optimum service. The server farm is responsible for the provision of security, protection, and high speed connectivity for the network.

2.5. The Enterprise Edge

This module provides connection to the service provider edge with the aid of its component, viz., the E-commerce, WAN, VPN and internet [47]. Part of the services provided are security, QoS, and policy enforcement when connections are extended to remote areas.

In addition to balancing traffic, a well-designed network minimizes the extent of failure domains. The region of a network that is affected when a crucial device or service malfunctions is known as the failure domain [46]. The effect of a failure domain, however, depends on the function of the device that breaks first.

2.6. The Service Provider Edge

The services provided by this module are WAN, public switched telephone network (PSTN), and internet [48]. Some of the resources outside the campus are connected through the service provider, which also streamlines communication to ISP and WAN.

3. Benefits of an Optimized Enterprise Network System

Nowadays, enterprises are embracing an all-encompassing, open networking approach that connects applications and IT systems across many network domains [29,49]. This interconnectivity facilitates better performance, efficient operations, enhanced security provisioning, and consistency across the whole enterprise. There are numerous benefits that can be derived when these services are optimally exploited.

3.1. Drive Towards Efficiency and Productivity

The effectiveness and productivity of an organization's numerous departments are greatly enhanced by a well-designed and reliable IT infrastructure [50]. Meeting project deadlines and the productivity of an employee are directly impacted by the seamless transfer of information, which in addition promotes quicker and more effective communications [51]. Apart from enhancing communication speed, an optimized enterprise network will guarantee improved client interactions through enhanced website functionality, online transactions, and interactive customer experiences.

3.2. Enhanced Security Provisioning

In order to detect security risks and cyber-attacks early, enterprise network optimization is crucial. With a well-developed network, a security vulnerability can be found quickly enough to stop extensive data compromise. Furthermore, in the event of hardware loss or breach of security, network optimization eliminates data manipulation, which promotes improved disaster management and speedy recovery [52,53].

Big businesses are striving for real-time detection of security threats for better monitoring and protection from attacks. An enterprise network serves as a main threat detector by implementing real-time security mechanisms to complement the roles of firewalls, secure internet gateways, and security applications [54]. Some of these functions are accomplished through profiling, access control, network monitoring, verification, and device management and identification.

3.3. Reduced IT Downtime

Incessant IT breakdowns, malfunctions, and downtime can cause businesses to suffer significant financial losses [50]. Organizations lose a lot of money with every outage or failure, and these unpleasant situations will occur more frequently in a company with obsolete and ineffective IT infrastructure. By optimizing the cloud-based IT infrastructure, a company can prevent considerable loss of revenue and in turn realize a huge increase in productivity [55]. Faster speed and greater network availability are outcomes of a strong and optimized network, which reduces downtime and employee frustration, while boosting productivity.

3.4. Cost Minimization

Reduced operational expenses are a direct result of an optimized enterprise network, since it drastically minimizes expenses for operations, services, software, hardware, and maintenance [56]. In addition, implementing cloud-based structures promotes efficient data management, improved corporate procedures, and smooth device interoperability [57]. Large enterprises may find it easier to benefit from network optimization, even though it is crucial for all kinds of businesses. Nonetheless, network optimization is very important for small organizations, as it will help them reduce cost, better manage revenue, and provide high-quality services.

3.5. Effective Cloud Integration

With the increasing development and delivery of data and applications across several public clouds, enterprise networks facilitate efficient communication between cloud-based applications and end users [58]. Enterprises anywhere can benefit from improved connectivity through cloud network integration, which will enable them to efficiently manage their operations and clients [59]. Additionally, it streamlines the real-time access to information and interaction between end users, internal staff, external stakeholders, and the network infrastructure.

4. Enterprise Network Functionality

The primary goal of enterprise networks for many years has always been to interconnect everyone and everything. All connections are routed to the self-hosted, on-premise centralized data centers, where programs are run and data are stored [60]. Users and devices can then be connected to the LAN in different branch offices to enable this access. The LAN in individual branch offices is connected to broader enterprise WAN using a dedicated multiprotocol label switching (MLSP) links [29,30].

Every layer facilitates an organized method of controlling network access and traffic, which eliminates bottlenecks, supports efficient data processing, and promotes effective management of security policies. All these processes are facilitated by different techniques in order to guarantee seamless interconnectivity.

4.1. Data Flow and Communication Protocols

Enterprise networks use transmission control protocol/internet protocol (TCP/IP) to transport data [61,62]. These protocols organize data into packets and route them from their source to destination. Switching and routing devices utilize dedicated protocols such as open shortest path first (OSPF), border gateway protocol (BGP), and ethernet to determine the optimal path for every packet. The aim is to guarantee a dependable data flow throughout the network [63].

4.2. Centralized Management with SDN

In the current enterprise networks, SDN becomes crucial since it separates physical hardware completely from network management [64]. Hence, a centralized control plane that can dynamically regulate the data flows throughout the network is supported by SDN. In addition, SDN enables managers to rapidly alter network resources, set security guidelines, and manage services in response to immediate demands via a centralized console. Thus, a tight integration of AI/ML technique via network orchestration can further strengthen SDN self-adaptation capabilities to satisfy IoT service conditions [65].

4.3. Embedded Security Architecture: Zero Trust and SASE

Nowadays, advanced security features have been integrated into enterprise networks to protect systems and data. Some of the important security mechanisms are zero trust network architecture (ZTNA) and secure access service edge (SASE).

4.3.1. Zero Trust Network Architecture

ZTNA is an enterprise cybersecurity framework that is based on 'never trust, always verify' principles. It is designed to reduce internal lateral movement and prevent data breaches. ZTNA protects data and services and minimizes unauthorized access by performing checks on network requests, based on an established access policy [7,8,66]. The type of access requests could range from enterprise applications, infrastructure components, devices, and virtual and cloud components. Hence, the ZTNA concept can broadly be seen as cybersecurity strategy for an organization that incorporates operational policies and network infrastructure (both virtual and physical). Based on the lateral movement of threats and zero trust assumptions, the network security can further be improved by incorporating micro-segmentation policy [67]. As shown in Figure 5, access will only be granted to an enterprise facility through a policy enforcement point (PEP) and a policy decision point (PDP) [8]. Thus, ZTN applies two basic functions of authentication and authorization through policy decision/ enhancement point (PDP/PEP) to grant access to any resources.

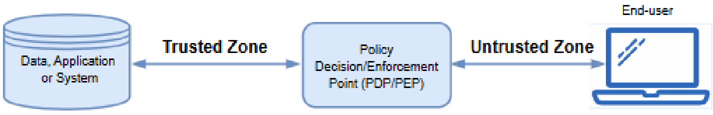
Data, Application or System
Trusted Zone
Policy Decision/Enforcement Point (PDP/PEP)
Untrusted Zone
End-user

Figure 5. Zero trust network architecture framework [8].

4.3.2. Secure Access Service Edge

The SASE is an emerging paradigm of cybersecurity, a cloud-based design that moves typical on-premise security and network connectivity to the cloud for proximity to data [5,68]. It ensures secure access for branch offices and remote users alike. Additional security is guaranteed by integrating software-defined WAN (SD-WAN) capabilities with network security features such as ZTNA [69], firewall-as-a-service (FWaaS) [70], secure web gateways (SWG), and cloud access security broker (CASB) [69]. In addition, SASE creates the convergence and integration of security functions and cloud-based connectivity [71]. As illustrated in Figure 6, it is important to note that SASE can be viewed beyond a single solution paradigm. Rather, as a platform for dynamically deploying network, data, application, cloud, and security structures for adaptability. Due to adaptability of SASE architecture, there is no restriction on what can be implemented.

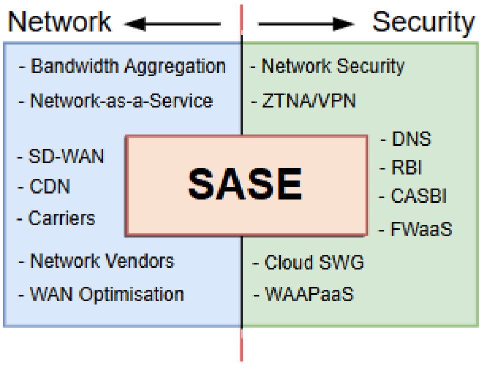

Figure 6. SASE model for security and network integration.

4.4. Cloud and Multi-Cloud Integration

In order to provide access to applications and services, enterprise networks frequently interact with both public and private cloud environments [37,72]. Secure application programming interface (API) gateways, dedicated links, or VPNs are commonly used to accomplish this task. With the help of multi-cloud approaches, or cloud systems, organizations can use services from several cloud providers to create a scalable and robust environment. A typical example is when a user or an organization has data stored on a private cloud, performs document sharing on, say, Google Cloud platform, and executea data analysis on another cloud application.

However, as businesses streamline their operations in multi-cloud environments, the need to ensure adequate security and resource management for optimal performance may arise. Thus, cloud providers can address security challenges by taking into account several factors. They include implementing identity and access management (IAM), controlling threats and vulnerabilities, and conducting comprehensive audit processes. These functions are embedded in federated access control, which hinges on creating relationships of trust between cloud and identity providers [73]. With federated access control, enterprises can be assured of adequate security without compromising network performance.

4.5. Network Monitoring and AI-Driven Analytics

Enterprise networks depend on AI-driven analytics and monitoring technologies to guarantee reliable performance and security [74]. Network managers are constantly alerted of any problems by network performance management (NPM) tools, which constantly track traffic patterns in order to identify abnormalities. Consequently, this process is improved by artificial intelligence (AI) and machine learning (ML) through identification of malicious patterns, activation of self-healing mechanisms [75–77], and prediction of bottlenecks within the network [1].

4.6. Network Virtualization and Cloud-Managed Networking

Network virtualization increases flexibility and scalability of enterprise networks. This is achieved through the deployment of several virtual networks on a shared physical infrastructure via VLANs and SD-WAN technologies [78]. Segmented traffic, especially for applications with different data and security needs, can be managed in this manner by various organizations. Furthermore, cloud-managed networking technologies simplify IT operations for distributed networks by allowing remote configuration and management.

Every technology, layer, and security approach in an enterprise network cooperates to guarantee movement of data freely and efficiently between devices and corresponding users [79]. In addition, cloud resources and branch and remote offices are all seamlessly incorporated into the core network to provide reliable, secure, and continuous access from any location. However, this continuous exchange of cloud resources across different platforms may lead to excessive consumption of energy. Thus, a green energy-saving computing solution, similar to the approach developed by [80], will prevent high energy consumption within the cloud-managed environment.

5. New Trends and Future Research Directions in Enterprise Networking

Enterprise networking has advanced in recent years as a result of emerging technologies and evolving business requirements. With the advent of cloud-native applications, overwhelming cybersecurity risks, and increasingly distributed work environments, new trends are committed to improving network agility, security, and management efficiency [81]. In the preceding sections, we have outlined how enterprise networking has evolved over the years as a promising tool that facilitates ease of communication in a business environment.

Also, we highlighted various benefits derived and challenges encountered from adopting these traditional techniques. Nonetheless, there are several other recent development strategies in enterprise networking. Notable amongst these are the adoption of state-of-the-art technologies such as software-defined wide area networks (SD-WAN) [82], network automation [83], AI-driven network management [1,74], hybrid and multi-cloud networking [37,72], and the increasing adoption of secure access service edge (SASE) and zero trust networking [5,7,66,68]. Table 1 summarizes the survey techniques and their classification into different performance-based interventions.

5.1. SD-WAN

SD-WAN has rapidly taken over as the standard WAN technology due to its increased flexibility, enhanced performance, and robust security [82,84,85]. Compared to traditional WANs, SD-WAN provides a layered architecture that is far simpler to run. It also offers a network design that transfers the management and control layers to the cloud via a centralized controller [86]. It is anticipated that there will be further adoptions and migrations from the conventional enterprise WAN technology to SD-WAN. Since SD-WAN does not rely on public lines, there is considerable reduction in cost due to utilization of public internet.

Utilizing SD-WAN optimizes the current IT infrastructure, increasing network capacity, decreasing latency, and improving network scalability. Organizations that have already embraced the technology will also concentrate on leveraging its extensive potentials. That is, by rationalizing their applications through the use of universal customer premises equipment (UCPE) and virtual network functions (VNFs) [85,87]. The network functions are separated into data, control, and application planes by SD-WAN (see Figure 7), in the same way as SDN.

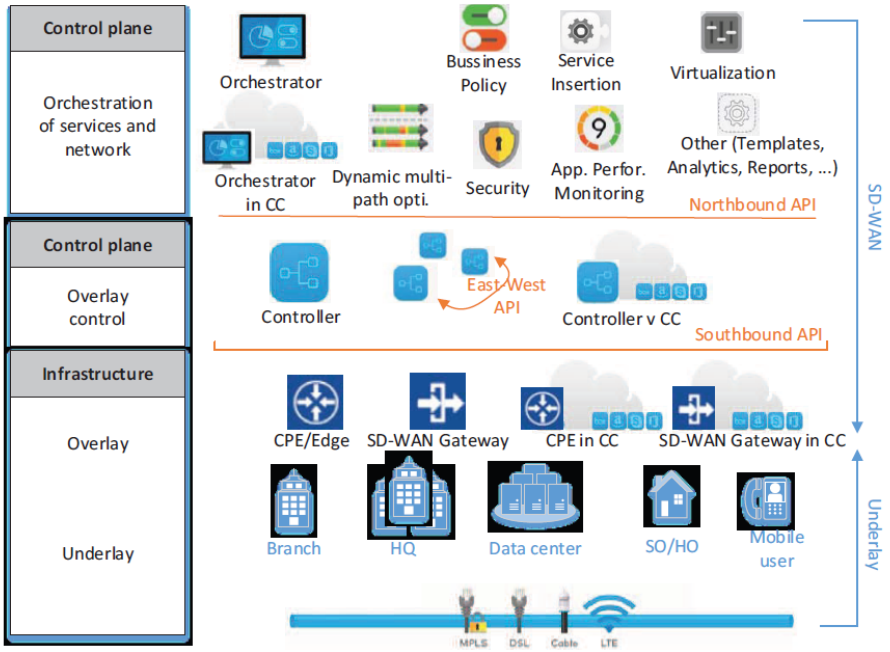

Figure 7. SD-WAN architecture [82].

The data plane transports application and user data, while the control plane performs system configuration, monitoring, and making routing decisions [82]. However, the application plane, commonly known as orchestration plane, leverages on the services provided by the control plane. Despite these benefits, SD-WAN technologies can be affected by limitations that impact network security and performance, especially in latency-sensitive applications. Some of them include configuration errors, software vulnerabilities, and interoperability and scalability problems. To address these challenges, ref. [88] proposed SD-WAN-based multi-objective networking improvement measures, such as new transport protocols, NFV, and ML for networking.

Table 1. Classification of survey techniques for enterprise networking optimization.

Category	Survey Techniques	Challenges	Solutions & Performance	Technological Interventions
Security-based Techniques	Intrusion Detection and Prevention (IDPS), VPNs	High false positive rates, low detection latency	AI-driven threat detection [53,54], automated mitigation, Improved WAN optimization [4,37,72]	Deep learning-based intrusion detection [6], early network monitoring tools [74]
	Zero Trust Network Architecture (ZTNA)	Implementation complexity, integration with legacy systems	Micro-segmentation [67], continuous authentication [8]	Cloud-native Zero Trust [81]
	Cybersecurity Mesh Architecture (CSMA)	Data inconsistency, real-time analysis difficulty	Data aggregation and tool integration [89], threat intelligence [90]	Threat-sharing platforms [91], federated learning for cybersecurity [39]
Cloud and SDN-based interventions	Cloud Networking	Security breaches, Cost management	Multi-cloud strategies [92], hybrid cloud security models [38]	Software-defined cloud networking, SASE [4,69]
	Software-Defined Networking (SDN)	Control plane vulnerabilities, compatibility issues	Open-source SDN controllers [93], policy-based automation [83]	AI-driven network orchestration [65], intent-based networking [94]
Cloud and SDN-based interventions	Software-Defined WAN (SD-WAN)	Complexity in deployment, security risks, high power consumption	AI-based traffic routing [95], AI-driven integrated security SASE [72], Energy-saving control [80], Ultra-low latency [88]	Cloud-native SD-WAN [84,85], Hybrid & Multi-cloud networking [37,38], AI-based optimization [75]
AI-Driven and Automation solutions	AI-based network Optimization	High computational costs, trustworthiness of AI decisions	Federated learning [39], cloud-based AI platforms [74]	Predictive analytics [75], real-time network self-healing [1,75]
	Edge Computing, Network automation	Difficult policy translation, scalability concerns	Adaptive control mechanisms [43]	AI-powered policy automation [96,97]
	Self-Healing Networks	Complexity in automation, fault prediction accuracy	Reinforcement learning models [77]	Autonomous networks & Self-configuring AI agents [76]

5.2. Network Automation

Since the emergence of SDN and NFV, the traditional static network has witnessed a significant transformation, opening the door for new network technologies. Another remarkable advancement is the automation and effective management of complicated networks through software for achieving optimal performance [83,98]. Large enterprises are using automated networks more frequently in an attempt to increase productivity and reduce operational expenses. Manual network management is becoming even less effective due to increasing global digitization, with challenges ranging from configuration or human error, to variations and IT outages. Thus, organizations will experience overall network efficiency with the use of AI and machine learning for network operations, providing the possibility of central or remote management [96,97].

Due to the manual nature of most network management tasks, performing regular maintenance on them has led to time consumption and wastage of resources. Network automation readily comes to the rescue, as these operations can be carried out more regularly and efficiently, thereby reducing the likelihood of network failure and downtime. Additionally, network automation provides easier ways to maintain network operations by applying configurations (in Figure 8) consistently with less effort across the infrastructure. However, with more connected devices and adoption of software-enabled management systems, the network is continuously exposed to a range of automation security threats. They include phishing attacks, insider threats, ransomware, and malware, among others. By identifying these vulnerabilities, more sophisticated approaches with threat hunting capabilities can be applied to complement other security interventions [99].

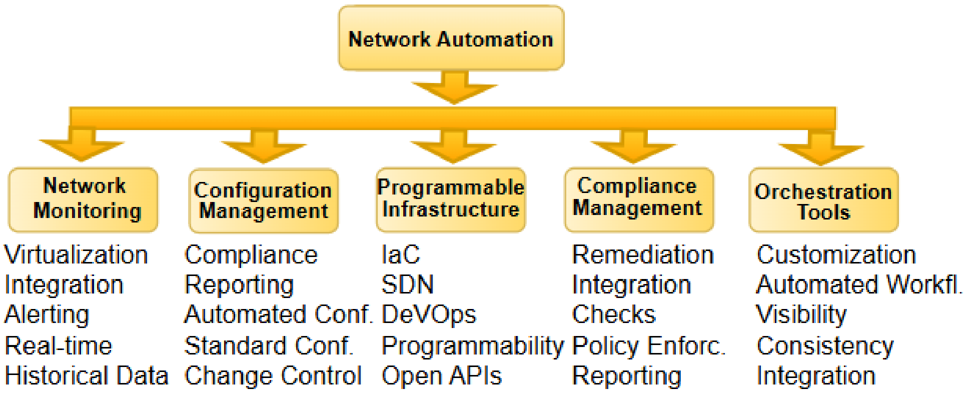

Figure 8. Network automation structure.

5.3. Hybrid and Multi-Cloud Networking

Several enterprise firms are seeking ways to integrate services from multiple cloud providers in order to achieve flexibility, resilience, and performance optimization [37,72]. This is apparent in the shift towards multi-cloud and hybrid networking. Hybrid networking promotes data sovereignty and low-latency access to essential applications by combining cloud services with on-premises infrastructure [57]. Networking solutions are developing as businesses implement multi-cloud strategies to offer smooth connectivity and control across various data centers and cloud providers. This will minimize latency and improve data security. Cloud computing, which integrates traditional technologies, enables computer functionalities to be accessed and managed remotely [92].

Therefore, cloud computing in hybrid, multi, public, or private connectivity modes permit computations and data processing to take place at data centers. Data centers possess significant amounts of data and computational capacity to transmit between different locations [100]. Consequently, clients only pay for storage, data transfer, or processing resources utilized at any instant time. This allows organizations to focus on other business goals without any concern about maintaining the computer hardware and infrastructure. Generally, as illustrated in Figure 9, cloud computing technologies can be deployed in the form of infrastructure-as-a-service (IaaS) [101], software-as-a-service (SaaS) [102], and platform-as-a-service (PaaS) [93] mode. These deployments use the respective infrastructure, software, and platform from the cloud to provide services in the form of rent to end users.

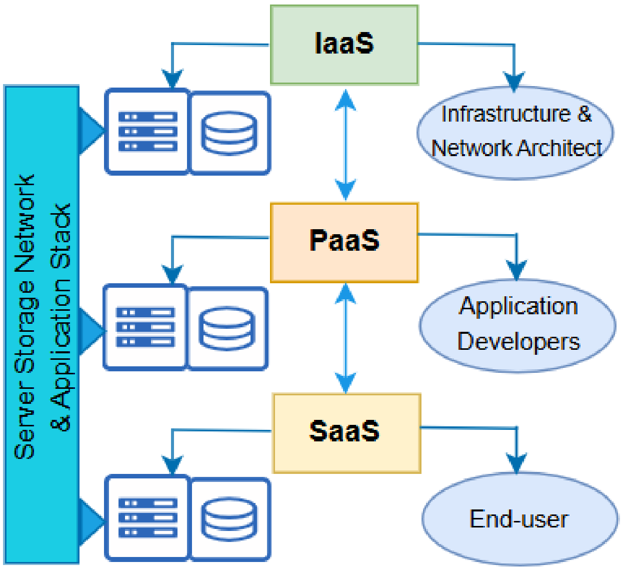
IaaS
PaaS
SaaS
Infrastructure & Network Architect
Application Developers
End-user
Server Storage Network & Application Stack

Figure 9. Cloud computing deployment model.

5.4. Network-as-a-Service (NaaS)

With network-as-a-service (NaaS), organizations can scale network services up or down according to their needs, attributed to its flexible, subscription-based networking paradigm [9,103]. Hence, NaaS streamlines networking by eliminating the need for capital expenditures and operational complexity. In addition, it separates infrastructure management, thereby enabling firms to rent network capabilities as required [104]. This pattern is consistent with a larger movement toward "as-a-service" models. For this reason, business firms can use specialized network services without the need for requisite knowledge, while concentrating on their core business operations. By utilizing enterprise 5G and cloud computing as the enabling technology, customized traffic flow can be created by NaaS to significantly improve the QoS requirements of diverse applications [95].

Also, the enterprise may easily incorporate new applications that require wider expansion, allowing for flexible organizational growth (see Figure 10). Hence, NaaS paradigm eliminates the need for the IT department to determine or have information about network activities. Rather, networks and IT share a common knowledge of network services by relying on the same set of open APIs [103]. This gives networking domains more freedom to decide how best to develop, guarantee, and control the visibility of a network function, such as firewall-as-a-service (FaaS). However, this also depends upon which options best meet the needs of clients.

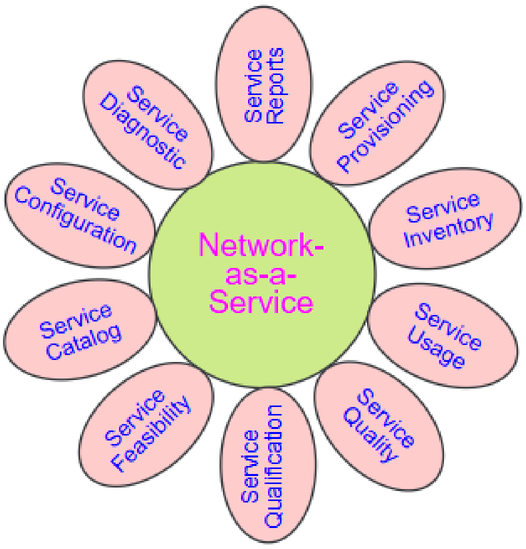

Figure 10. NaaS management and service functions.

5.5. Edge Computing and 5G Integration

Edge computing is becoming an essential component of enterprise networking due to the explosion of Internet of Things (IoT) devices and the demand for real-time data [91,105]. With the proliferation of data usage across various fields, the entire world is gradually drifting towards digitalization. Edge computing lowers latency and preserves bandwidth by processing data closer to its source. This will ultimately promote optimal performance of sectors such as finance, healthcare, and manufacturing that rely on quick responses.

The adoption of 5G networks further enhances edge computing, since it offers low-latency and high-speed connectivity [106,107]. This helps to facilitate quicker data transfer between devices, enabling decision-making and real-time analytics closer to the data source, as illustrated in Figure 11. While cloud technology proves to be very efficient in data processing, the bandwidth required to send data limits its application. Hence, edge computing readily emerges to remedy the data transfer bottleneck regularly encountered by cloud computing during computation [108,109]. However, it is noteworthy that edge computing also performs the function of a data producer in addition to data consumer role at the cloud.

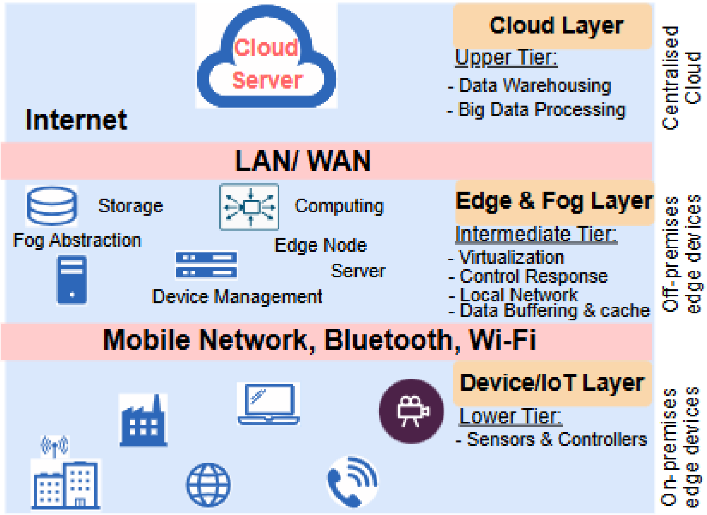

Figure 11. Illustration of edge computing architecture and example.

The edge computing architecture is categorized in Table 2 based on the deployment types and roles played for the successful implementation of its objectives. In addition, some software platforms, such as virtualization, data analytics [19], and edge orchestration, help to simplify the complex nature of edge computing.

Table 2. Key features and characteristics of edge computing architecture [109].

	Edge Computing Architecture Layer			
Characteristics	**IoT**	**Edge**	**Fog**	**Cloud**
Data	Source	Process	Process	Process
Storage Limits	Extremely Limited	Limited	Limited	Unlimited
Deployment	Distributed	Distributed	Distributed	Centralized
Components	Physical devices	Edge Nodes	Fog Nodes	Virtual Cloud res.
Response Time	No response time	The fastest	Fast	Slow
Location awareness	Aware	Aware	Aware	Aware
Nodes Count	The largest	Very large	Large	Small
Computational limits	Limited	Limited	Limited	Unlimited
Data source distance	The source	The nearest	Near	Far

5.6. Cybersecurity Mesh Architecture (CSMA)

Cybersecurity means protecting the software, hardware, network, and data from unauthorized access and accidental attack or damage. Since its inception, the field of cybersecurity has developed to be dynamic and challenging [89,90]. Currently, CSMA includes a variety of tools and techniques, functioning to protect systems, networks, and data from a broad range of cyber threats. Figure 12 shows CSMA architecture and different aggregated layers. With every new security solution, there are more ways for attackers to penetrate past existing security features. Thus, CSMA proves to be of great advantage to large organizations by relying on data aggregation and tool integration approaches [110].

Each layer of CSMA platform can communicate with the layers above and below it by grouping existing security and analysis devices into stratified layers. As a result, a functional structure is created that enables communication and cooperation amongst highly distributed networks. Security activities are therefore made more efficient by the centralized dashboards and controls that receive all of this information. Additionally, CSMA features AI-supported automation and unified threat intelligence awareness to create a dynamic security system that can circumvent potential attackers [89]. Modern enterprise requires a network to connect its on-premises servers, cloud services, tools, and home and edge devices [111]. Therefore, network security revolves around protecting these geographically distributed resources.

In summary, much has been discussed about advancements in enterprise networking which are shaping the current landscape. Other technologies such as artificial intelligence (AI)-powered IBN architecture [94]; Wi-Fi 6; its successor, Wi-Fi 7; or IEEE 802.11be and beyond 5G (B5G) networks [112,113] are the latest technologies provisioned to deliver seamless wireless access for businesses. They possess the advantage of providing higher bandwidth and supporting more users per access point. These cutting-edge wireless solutions have been optimized to provide ultra-fast speed compared to wired access architecture. With Wi-Fi 7, more connected users and devices are supported without affecting performance, while allowing data to move securely over wireless networks.

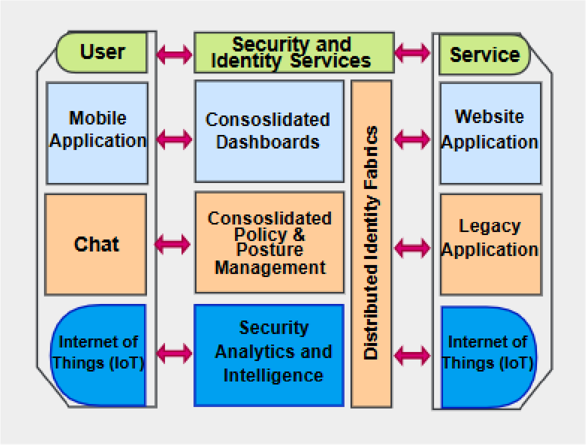

Figure 12. Cybersecurity mesh architecture and layers.

6. Conclusions

This paper provided a comprehensive survey of state-of-the art technologies and trends in enterprise networking. The significant attraction gained by enterprise networking as gateway to optimized business solutions has necessitated the urgent need for appraisal of conventional network technologies. Hence, the architectural composition was first considered in order to give an idea of the strategic importance of enterprise networking in ensuring seamless connectivity between users and devices. We then presented various benefits of enterprise networking in terms of profit maximization and enhanced security and productivity. At the same time, we appraised dedicated converged techniques of network and security solutions aimed towards achieving advanced hybrid cloud environments.

Therefore, in achieving its status as a unique contribution to the literature, this paper not only presented a detailed overview of both traditional and contemporary trends in enterprise networking, but also provided specific direction for researchers to identify potential areas of improvement, especially in terms of security and performance.

Author Contributions: O.A.: Conceptualization, Literature Review, Analysis of Existing Works and Writing of the original draft. M.S.T.: Supervision, and Review on writing and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No data were created during the conduct of this research.

Acknowledgments: We would like to thank the editor and reviewers for their professional advice and valuable feedback which have significantly contributed to the quality of this review. Also, we would like to thank the Federal Polytechnic, Ede, Nigeria for the support given.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
API	Application Programming Interface
ASN	Autonomous System Number
BGP	Border Gateway Protocol
CASB	Cloud Access Security Broker
CSMA	Cybersecurity Mesh Architecture

ECNM	Enterprise Composite Network Model
FaaS/FWaaS	Firewall-as-a-Service
IaaS	Infrastructure-as-a-Service
IAM	Identity and Access Management
ISP	Internet Service Provider
IoT	Internet of Things
IT	Information Technology
LAN	Local Area Network
ML	Machine Learning
MPLS	Multiprotocol Label Switching
NaaS	Network-as-a-Service
NPM	Network Performance Management
OSPF	Open Shortest Path First
PaaS	Platform-as-a-Service
PDP/PEP	Policy Decision/Enhancement Point
PSTN	Public Switched Telephone Network
QoS	Quality of Service
SaaS	Software-as-a-Service
SASE	Secure Access Service Edge
SDN	Software-Defined Networking
SD-WAN	Software-Defined Wide Area Network
SWG	Secure Web Gateway
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UCPE	Universal Customer Pemises Equipment
VLANs	Virtual LANs
VPNs	Virtual Private Networks
WAN	Wide Area Network
ZTNA	Zero Trust Network Access

References

1. Prangon, N.F.; Wu, J. AI and Computing Horizons: Cloud and Edge in the Modern Era. *J. Sens. Actuator Netw.* **2024**, *13*, 44. [CrossRef]
2. Eshmurodov, A. Innovations in IT: Shaping the Future of Digital Transformation. *Am. J. Eng. Mech. Archit.* **2024**, *2*, 118–125.
3. Wehner, B.; Ritter, C.; Leist, S. Enterprise social networks: A literature review and research agenda. *Comput. Netw.* **2017**, *114*, 125–142. [CrossRef]
4. Nadaf, S.M.; Rath, H.K.; Simha, A. A novel approach for an enterprise network transformation and optimization. In Proceedings of the 2012 Annual IEEE India Conference (INDICON), Kochi, India, 7–9 December 2012; pp. 317–322.
5. Velayutham, A. Secure Access Service Edge (SASE) Framework in Enhancing Security for Remote Workers and Its Adaptability to Hybrid Workforces in the Post-Pandemic Workplace Environment. *Int. J. Soc. Anal.* **2023**, *8*, 21.
6. Sathupadi, K. A hybrid deep learning framework combining on-device and cloud-based processing for cybersecurity in mobile cloud environments. *Int. J. Inf. Cybersecur.* **2023**, *7*, 61–80.
7. Zohaib, S.M.; Sajjad, S.M.; Iqbal, Z.; Yousaf, M.; Haseeb, M.; Muhammad, Z. Zero Trust VPN (ZT-VPN): A Systematic Literature Review and Cybersecurity Framework for Hybrid and Remote Work. *Information* **2024**, *15*, 734. [CrossRef]
8. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. *Zero Trust Architecture*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020. [CrossRef]
9. Chandramouli, R.; Chandramouli, R. *Guide to a Secure Enterprise Network Landscape*; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2022.
10. Souppaya, M.; Scarfone, K. Guide to enterprise telework, remote access, and bring your own device (BYOD) security. *NIST Spec. Publ.* **2016**, *800*, 46.
11. Shin, B. *A Practical Introduction to Enterprise Network and Security Management*; Auerbach Publications: Boca Raton, FL, USA, 2021.
12. Iskandar, A.I.; Arham, A.F.; Shohaime, N. The use of social media, e-mail and instant messaging as the predictors of an employee's work performance. *J. Acad.* **2017**, *5*, 127–136.

13. Cascio, W.F.; Montealegre, R. How technology is changing work and organizations. *Annu. Rev. Organ. Psychol. Organ. Behav.* **2016**, *3*, 349–375. [CrossRef]
14. Raza, M. Enterprise Networking Explained: Types, Concepts and Trends. 2021. Available online: https://www.bmc.com/blogs/enterprise-networking/ (accessed on 16 December 2024).
15. Wen, Y. Enterprise IP LAN/WAN Design, The System Admin. Company (TAOS), Version 1.1, 2001; p. 26. Available online: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=0b3bc2def28f31309c0cb3250576bbf0be29b45a (accessed on 16 December 2024).
16. Iftikhar, A.; Qureshi, K.N.; Shiraz, M.; Albahli, S. Security, trust and privacy risks, responses, and solutions for high-speed smart cities networks: A systematic literature review. *J. King Saud-Univ.-Comput. Inf. Sci.* **2023**, *35*, 101788. [CrossRef]
17. Lv, H.; Zhang, Y.; Li, H.; Chang, W. Security Assessment of Enterprise Networks Based on Analytic Network Process and Evidence Theory. In Proceedings of the 2021 3rd International Conference on Artificial Intelligence and Advanced Manufacture (AIAM), Manchester, UK, 23–25 October 2021; pp. 305–313.
18. Hosam, O.; Abousamra, R.; Hassouna, M.; Azzawi, R. Security Analysis and Planning for Enterprise Networks: Incorporating Modern Security Design Principles. In *Industry 4.0 Key Technological Advances and Design Principles in Engineering, Education, Business, and Social Applications*; CRC Press: Boca Raton, FL, USA, 2024; pp. 85–117.
19. Palanivel, K. Modern network analytics architecture stack to enterprise networks. *Int. J. Res. Appl. Sci. Eng. Technol. (IJRASET)* **2019**, *7*, 2634–2651. [CrossRef]
20. Weerasinghe, B. *Modern Network Management and Security within Large Enterprise Network*; University of Sri Jayewardenepura: Nugegoda, Sri Lanka , 2020; p. 5.
21. Onu, F.; C, I. Comparative Study of Optic Fibre and Wireless Technologies in Internet Connectivity. *Int. J. Comput. Appl. Technol. Res.* **2016**, *5*, 403–411. [CrossRef]
22. Jyothi, K.K.; Reddy, B.I. Study on virtual private network (VPN), VPN's protocols and security. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.* **2018**, *3*, 919–932.
23. Nemmi, E.N.; Sassi, F.; La Morgia, M.; Testart, C.; Mei, A.; Dainotti, A. The parallel lives of autonomous systems: ASN allocations vs. BGP. In Proceedings of the the 21st ACM Internet Measurement Conference, Virtual Event, 2–4 November 2021; pp. 593–611.
24. Awasthi, A. Network Classification for an Enterprise. *Int. J. Sci. Res. (IJSR)* **2020**, *9*, 635–637.
25. Seneviratne, S.; de Silva, R. Framework for Enterprise Local Area Network Design: An Object-Connectivity Approach. In Proceedings of the 10th International Conference on Information Technology Convergence and Services (ITCSE 2021), Sydney, Australia, 26–27 June 2021 ; Volume 11.
26. Mo, Z. Small and Medium-Sized Enterprise Office LAN Construction Scheme. In Proceedings of the International Conference on Education, Management, Computer and Society, Shenyang, China, 1–3 January 2016 ; Atlantis Press: Dordrecht, The Netherlands, 2016; pp. 1149–1151.
27. Dr, N.; Hussain, R. A exploration of Multi-Protocol Label Switching (MPLS) network: A review. *J. Crit. Rev.* **2020**, *7*, 2664–2671.
28. Srivastava, S.; Singh, J.P. Efficiency of Multi-Protocol LABEL Switching over Traditional Switching. In Proceedings of the 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 22–23 October 2021; pp. 1–4.
29. Goutam, S.; Goutam, A. Recent Trends in Deployment of Multi-Protocol Label Switching (MPLS) Networks in Universities. In *Global Higher Education Practices in Times of Crisis: Questions for Sustainability and Digitalization*; Emerald Publishing Limited: Bingley, UK, 2024; pp. 255–269.
30. Saxena, R.; Patel, A.S. Generalized Multi-protocol Label Switching based Virtualization for Cloud Computing. In Proceedings of the 2022 International Conference on Connected Systems & Intelligence (CSI), Trivandrum, India, 31 August–2 September 2022; pp. 1–8.
31. Mwape, J.C. Performance Evaluation of Internet Protocol Security (IPSec) over Multiprotocol Label Switching (MPLS). Ph.D. Thesis, The University of Zambia, Lusaka, Zambia, 2024.
32. Guo, Y. *Transformation from On-Premise Software to Cloud Computing-Based Services: A Case Study of SAP Practices*; The University of Manchester (United Kingdom): Manchester, UK, 2021.
33. Wescott, A.P. *Analysis of On-Premise Data Center Transition*; Capitol Technology University: Laurel, MD, USA, 2020.
34. Khan, H.U.; Samad, H.S.I.A. Enterprise strategic shift of technology: Cloud-based systems verses traditional distributed system. *Int. J. Enterp. Netw. Manag.* **2020**, *11*, 320–346. [CrossRef]
35. Kajati, E.; Papcun, P.; Liu, C.; Zhong, R.Y.; Koziorek, J.; Zolotova, I. Cloud based cyber-physical systems: Network evaluation study. *Adv. Eng. Inform.* **2019**, *42*, 100988. [CrossRef]
36. Ganesh, C.; Saran, A.; Flora, G.D.; Saravanan, M. A cloud-based router management system for enterprise network management. In Proceedings of the 2022 International Conference on Computer, Power and Communications (ICCPC), Chennai, India, 14–16 December 2022; pp. 153–157.

37. Nair, R.R.; Sreevidya, D.; Mohan, C.R.; Banerjee, J.; Chouhan, K.; Dharamvir. Comprehensive Approaches to Securing Multi-Cloud Architectures: Best Practices and Emerging Solutions. In Proceedings of the 2024 IEEE 7th International Conference on Contemporary Computing and Informatics (IC3I), Greater Noida, India, 18–20 September 2024; pp. 1631–1636.
38. Maxwell, R. The Challenges of Enterprise-Scale Hybrid and Multi-cloud Architectures. In *Azure Arc Systems Management: Governance and Administration of Multi-Cloud and Hybrid IT Estates*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 1–13.
39. Merseedi, K.J.; Zeebaree, S.R. The cloud architectures for distributed multi-cloud computing: A review of hybrid and federated cloud environment. *Indones. J. Comput. Sci.* **2024**, *13*. [CrossRef]
40. Shukla, A.; Patel, J.; Panzade, K.; Sardana, H. *Cisco Cloud Infrastructure*; Cisco Press: San Jose, CA, USA, 2023.
41. Alsowail, R.A.; Al-Shehari, T. A multi-tiered framework for insider threat prevention. *Electronics* **2021**, *10*, 1005. [CrossRef]
42. CCNA Discovery Learning Guide. Designing and Supporting Computer Networks 2008. Available online: https://ptgmedia.pearsoncmg.com/images/9781587132117/samplepages/1587132117_Sample.pdf (accessed on 16 December 2024).
43. Karakus, M.; Durresi, A. A survey: Control plane scalability issues and approaches in software-defined networking (SDN). *Comput. Netw.* **2017**, *112*, 279–293. [CrossRef]
44. da Costa Cordeiro, W.L.; Marques, J.A.; Gaspary, L.P. Data plane programmability beyond openflow: Opportunities and challenges for network and service operations and management. *J. Netw. Syst. Manag.* **2017**, *25*, 784–818.
45. Hamroz, M. Enterprise Campus Design: Multilayer Architectures and Design Principles, 2023; p. 77. Available online: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2023/pdf/BRKENS-2031.pdf (accessed on 16 December 2024).
46. Reid, A.; Lorenz, J.; Schmidt, C.A. *Introducing Routing and Switching in the Enterprise, CCNA Discovery Learning Guide*; Cisco Press: San Jose, CA, USA, 2008.
47. Academy, C.N. *Connecting Networks Companion Guide*; WebEx Communications; Pearson Education: London, UK, 2014; p. 576.
48. Communications, T. What Is a Core Network and How Does It Work? 2024. Available online: https://www.tatacommunications.com/knowledge-base/network-core-network-explained/ (accessed on 16 December 2024).
49. Andrieiev, O. Enterprise Networking Explained: Type, Benefits and Trends. 2024. Available online: https://jelvix.com/blog/what-is-enterprise-networking (accessed on 12 March 2025).
50. Ayegba, J.O.; Lin, Z.L. An overview on enterprise networks and company performance. *Int. Entrep. Rev.* **2020**, *6*, 7–16.
51. Nikitina, N. The concept of increasing the efficiency of the enterprise in modern conditions. *E3S Web Conf.* **2023**, *389*, 09003.
52. Rashmi Shree, V.; Antony, Z.C.; Jayapandian, N. Enhanced Data Security Architecture in Enterprise Networks. In Proceedings of the International Conference on Computer Networks, Big Data and IoT (ICCBI-2018), Madurai, India, 19–20 December 2018; pp. 857–864.
53. Lyu, M.; Gharakheili, H.H.; Sivaraman, V. A survey on enterprise network security: Asset behavioral monitoring and distributed attack detection. *IEEE Access* **2024**, *12*, 89363–89383.
54. Mishra, A. *Modern Cybersecurity Strategies for Enterprises: Protect and Secure Your Enterprise Networks, Digital Business Assets, and Endpoint Security with Tested and Proven Methods (English Edition)*; BPB Publications: Noida, India, 2022.
55. Wang, S.S.; Franke, U. Enterprise IT service downtime cost and risk transfer in a supply chain. *Oper. Manag. Res.* **2020**, *13*, 94–108.
56. Osemwengie, L.; Jafari, F.; Karami, A. Designing a Cost-Efficient Network for a Small Enterprise. In *Intelligent Computing: Proceedings of the 2021 Computing Conference, Volume 1*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 255–273.
57. Mollahoseini Ardakani, M.R.; Hashemi, S.M.; Razzazi, M. A cloud-based solution/reference architecture for establishing collaborative networked organizations. *J. Intell. Manuf.* **2019**, *30*, 2273–2289.
58. Jia, D.; Wu, Z. Enterprise collaborative integrated management system based on IoT cloud technology. *Mob. Inf. Syst.* **2022**, *2022*, 6098201.
59. Fernando, C. Building Enterprise Software Systems with Hybrid Integration platforms. In *Solution Architecture Patterns for Enterprise: A Guide to Building Enterprise Software Systems*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 109–146.
60. Lowe, S.D.; Green, J.; Davis, D. *Building a Modern Data Center*; ActualTech Media: Bluffton, SC, USA, 2016; pp. 103–157.
61. Nath, P.B.; Uddin, M.M. Tcp-ip model in data communication and networking. *Am. J. Eng. Res.* **2015**, *4*, 102–107.
62. Miajee, M.R.K. Network layer: TCP/IP Model. *Am. Int. J. Sci. Eng. Res.* **2018**, *1*, 22–25.
63. Shahid, K.; Ahmad, S.N.; Rizvi, S.T.H. Optimizing Network Performance: A Comparative Analysis of EIGRP, OSPF, and BGP in IPv6-Based Load-Sharing and Link-Failover Systems. *Future Internet* **2024**, *16*, 339. [CrossRef]
64. Nisar, K.; Jimson, E.R.; Hijazi, M.H.A.; Welch, I.; Hassan, R.; Aman, A.H.M.; Sodhro, A.H.; Pirbhulal, S.; Khan, S. A survey on the architecture, application, and security of software defined networking: Challenges and open issues. *Internet Things* **2020**, *12*, 100289.
65. Bernini, G.; Piscione, P.; Seder, E. AI-driven Service and Slice Orchestration. In *Shaping the Future of IoT with Edge Intelligence*; River Publishers: Aalborg, Denmark, 2024; p. 15.
66. Yan, X.; Wang, H. Survey on zero-trust network security. In Proceedings of the Artificial Intelligence and Security: 6th International Conference, ICAIS 2020, Hohhot, China, 17–20 July 2020; Proceedings, Part I 6; Springer: Berlin/Heidelberg, Germany, 2020; pp. 50–60.

67. Basta, N.; Ikram, M.; Kaafar, M.A.; Walker, A. Towards a zero-trust micro-segmentation network security strategy: An evaluation framework. In Proceedings of the NOMS 2022–2022 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 25–29 April 2022; pp. 1–7.
68. Seiffert, A. Secure Access Service Edge (SASE): Transforming Network and Security 2021; p. 17. Available online: https://www.cancom.at/_Resources/Persistent/f83d7d9927c6003fb271aaa16fe9f8a859475c0d/PaloAltoExpertForum_SASE%203.0.pdf (accessed on 12 March 2025).
69. Yiliyaer, S.; Kim, Y. Secure access service edge: A zero trust based framework for accessing data securely. In Proceedings of the 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 26–29 January 2022; pp. 0586–0591.
70. Fopa Mamene, M. Secure Access Service Edge (SASE): Architecture, Implementation and Performance Evaluation. Ph.D. Thesis, Hochschule Rhein-Waal, Kleve, Germany, 2024.
71. Huang, J.; Sun, J.; Yuan, X.; Zheng, Z. Intelligent Connectivity Solution for Enterprise Networking Services. In Proceedings of the 3rd International Conference on Digital Economy and Computer Application (DECA 2023), Shanghai, China, 22–24 September 2023; Atlantis Press: Dordrecht, The Netherlands, 2023; pp. 660–668.
72. Gundu, S.R.; Panem, C.A.; Thimmapuram, A. Hybrid IT and multi cloud an emerging trend and improved performance in cloud computing. *SN Comput. Sci.* **2020**, *1*, 256.
73. Dickinson, M.; Debroy, S.; Calyam, P.; Valluripally, S.; Zhang, Y.; Antequera, R.B.; Joshi, T.; White, T.; Xu, D. Multi-cloud performance and security driven federated workflow management. *IEEE Trans. Cloud Comput.* **2018**, *9*, 240–257.
74. Li, F.; Xu, G. AI-driven customer relationship management for sustainable enterprise performance. *Sustain. Energy Technol. Assess.* **2022**, *52*, 102103.
75. Papaioannou, A.; Dimara, A.; Kouzinopoulos, C.S.; Krinidis, S.; Anagnostopoulos, C.N.; Ioannidis, D.; Tzovaras, D. LP-OPTIMA: A Framework for Prescriptive Maintenance and Optimization of IoT Resources for Low-Power Embedded Systems. *Sensors* **2024**, *24*, 2125. [CrossRef] [PubMed]
76. Dimara, A.; Vasilopoulos, V.G.; Papaioannou, A.; Angelis, S.; Kotis, K.; Anagnostopoulos, C.N.; Krinidis, S.; Ioannidis, D.; Tzovaras, D. Self-healing of semantically interoperable smart and prescriptive edge devices in IoT. *Appl. Sci.* **2022**, *12*, 11650. [CrossRef]
77. Avgeris, M.; Leivadeas, A.; Lambadaris, I. A reinforcement-learning self-healing approach for virtual network function placement. In Proceedings of the NOMS 2023–2023 IEEE/IFIP Network Operations and Management Symposium, Miami, FL, USA, 8–12 May 2023; pp. 1–5.
78. Fowler, B. Cloud network engineering. In *AWS for Public and Private Sectors: Cloud Computing Architecture for Government and Business*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 23–41.
79. Anicho, O.; Abdullah, T. Impact of Cloud-based Infrastructure on Telecom Managed Services Models. *Data Sci. J. Comput. Appl. Inform.* **2020**, *4*, 71–88.
80. Saxena, S.; Khan, M.Z.; Singh, R. Green computing: An era of energy saving computing of cloud resources. *Int. J. Math. Sci. Comput.* **2021**, *7*, 42–48.
81. Tomar, M.; Ramalingam, S.; Krishnaswamy, P. Cloud-Native Enterprise Platform Engineering: Building Scalable, Resilient, and Secure Cloud Architectures for Global Enterprises. *Aust. J. Mach. Learn. Res. Appl.* **2023**, *3*, 601–639.
82. Segeč, P.; Moravčik, M.; Uratmová, J.; Papán, J.; Yeremenko, O. SD-WAN-architecture, functions and benefits. In Proceedings of the 2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA), Košice, Slovenia, 12–13 November 2020; pp. 593–599.
83. Arzo, S.T.; Naiga, C.; Granelli, F.; Bassoli, R.; Devetsikiotis, M.; Fitzek, F.H. A theoretical discussion and survey of network automation for IoT: Challenges and opportunity. *IEEE Internet Things J.* **2021**, *8*, 12021–12045.
84. Troia, S.; Zorello, L.M.M.; Maralit, A.J.; Maier, G. SD-WAN: An open-source implementation for enterprise networking services. In Proceedings of the 2020 22nd International Conference on Transparent Optical Networks (ICTON), Bari, Italy, 19–23 July 2020; pp. 1–4.
85. Troia, S.; Zorello, L.M.M.; Maier, G. SD-WAN: How the control of the network can be shifted from core to edge. In Proceedings of the 2021 International Conference on Optical Network Design and Modeling (ONDM), Gothenburg, Sweden, 28 June–1 July 2021; pp. 1–3.
86. Wang, J.; Bewong, M.; Zheng, L. SD-WAN: Hybrid Edge Cloud Network between Multi-site SDDC. *Comput. Netw.* **2024**, *250*, 110509.
87. Ashok, P.; Hallur, G. Demystifying Domain-Specific Key Drivers in Telecom Technologies. In Proceedings of the 2023 Intelligent Computing and Control for Engineering and Business Systems (ICCEBS), Chennai, India, 14–15 December 2023; pp. 1–9.
88. Qin, Z. SD-WAN for Bandwidth and Delay Improvements on the Internet. In *SHS Web of Conferences*; EDP Sciences: Les Ulis, France, 2022; Volume 144, p. 02004.
89. Sullivan, D. *Cybersecurity Mesh Architecture For Dummies, Fortinet Special Edition*; Fortinet Publication: Sunnyvale, CA, USA, 2023.

90. McLaughlin, K. Interweaving the Strands of AI and soar onto the Cybersecurity Mesh: A deep dive into the Cybersecurity Mesh and its role in modern digital defense strategies. *EDPACS*, **2023**, *68*, 27–33. [CrossRef]
91. Dias, I.; Ruan, L.; Ranaweera, C.; Wong, E. From 5G to beyond: Passive optical network and multi-access edge computing integration for latency-sensitive applications. *Opt. Fiber Technol.* **2023**, *75*, 103191. [CrossRef]
92. Hong, J.; Dreibholz, T.; Schenkel, J.A.; Hu, J.A. An overview of multi-cloud computing. In *Web, Artificial Intelligence and Network Applications: Proceedings of the Workshops of the 33rd International Conference on Advanced Information Networking and Applications (WAINA-2019) 33*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 1055–1068.
93. Saraswat, M.; Tripathi, R. Cloud computing: Analysis of top 5 CSPs in SaaS, PaaS and IaaS platforms. In Proceedings of the 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), Moradabad, India, 4–5 December 2020; pp. 300–305.
94. Njah, Y.; Leivadeas, A.; Falkner, M. An AI-driven intent-based network architecture. *IEEE Commun. Mag.* **2024**, 1–8. . [CrossRef]
95. Huang, T.; Tan, S.; Tang, Q.; Zhang, C.; Xie, R.; Yu, F.R. NT-SCDC: Realizing Service Customized Networking in Distributed Clouds with NaaS Ticket. *IEEE Netw.* **2023**, *38*, 236–243.
96. Rehman, Z.; Tariq, N.; Moqurrab, S.A.; Yoo, J.; Srivastava, G. Machine learning and internet of things applications in enterprise architectures: Solutions, challenges, and open issues. *Expert Syst.* **2024**, *41*, e13467.
97. Nozari, H.; Ghahremani-Nahr, J.; Szmelter-Jarosz, A. AI and machine learning for real-world problems. In *Advances In Computers*; Elsevier: Amsterdam, The Netherlands, 2024; Volume 134, pp. 1–12.
98. Chi, H.R.; Wu, C.K.; Huang, N.F.; Tsang, K.F.; Radwan, A. A survey of network automation for industrial internet-of-things toward industry 5.0. *IEEE Trans. Ind. Inform.* **2022**, *19*, 2065–2077.
99. Nour, B.; Pourzandi, M.; Debbabi, M. A survey on threat hunting in enterprise networks. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 2299–2324.
100. Krishnasamy, E.; Varrette, S.; Mucciardi, M. Edge computing: An overview of framework and applications. In *PRACE Technical Report*; PRACE aisbl: Bruxelles, Belgium, 2020.
101. Kashif, U.A.; Memon, Z.A.; Siddiqui, S.; Balouch, A.R.; Batra, R. Architectural design of trusted platform for IaaS cloud computing. In *Cloud Security: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2019; pp. 393–411.
102. Aleem, S.; Ahmed, F.; Batool, R.; Khattak, A. Empirical investigation of key factors for saas architecture. *IEEE Trans. Cloud Comput.* **2019**, *9*, 1037–1049.
103. Salas, G.D. Introduction to the Network Virtual Deployment for NaaS. 2022. Available online: https://hal.science/hal-03634559v1 (accessed on 12 March 2025).
104. Globa, L.; Sulima, S.; Romanov, O.; Skulysh, M. Dynamic Reconfiguration of Computing Resources to Support NaaS Technology. In *Proceedings of the International Conference on Applied Innovation in IT*; Anhalt University of Applied Sciences: Köthen, Germany, 2023; Volume 11, pp. 17–22.
105. Hassan, N.; Yau, K.L.A.; Wu, C. Edge computing in 5G: A review. *IEEE Access* **2019**, *7*, 127276–127289.
106. Liu, Y.; Peng, M.; Shou, G.; Chen, Y.; Chen, S. Toward edge intelligence: Multiaccess edge computing for 5G and Internet of Things. *IEEE Internet Things J.* **2020**, *7*, 6722–6747. [CrossRef]
107. Pham, Q.V.; Fang, F.; Ha, V.N.; Piran, M.J.; Le, M.; Le, L.B.; Hwang, W.J.; Ding, Z. A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art. *IEEE Access* **2020**, *8*, 116974–117017. [CrossRef]
108. Liyanage, M.; Porambage, P.; Ding, A.Y.; Kalla, A. Driving forces for multi-access edge computing (MEC) IoT integration in 5G. *ICT Express* **2021**, *7*, 127–137. [CrossRef]
109. Al-Dulaimy, A.; Sharma, Y.; Khan, M.G.; Taheri, J. Introduction to edge computing. In *Edge Computing: Models, Technologies and Applications*; Institution of Engineering and Technology: London, UK, 2020; pp. 3–25.
110. Ramos-Cruz, B.; Andreu-Perez, J.; Martínez, L. The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research. *Neurocomputing* **2024**, *581*, 127427. [CrossRef]
111. Tank, B.; Gandhi, V. A Comparative Study on Cloud Computing, Edge Computing and Fog Computing. In *Recent Developments in Electronics and Communication Systems*; IOS Press: Clifton, VA, USA, 2023; pp. 665–670.
112. Mozaffariahrar, E.; Theoleyre, F.; Menth, M. A survey of Wi-Fi 6: Technologies, advances, and challenges. *Future Internet* **2022**, *14*, 293. [CrossRef]
113. Morais, D.H. *5G NR, Wi-Fi 6, and Bluetooth LE 5: A Primer on Smartphone Wireless Technologies*; Springer Nature: Berlin/Heidelberg, Germany, 2023.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.