Deep Science Publishing
https://doi.org/10.70593/978-93-49910-67-6_12

Chapter 12: Preparing for what's next: Future-proofing networks for artificial intelligence, IoT, and smart infrastructure

12.1. Introduction

Securing a sustainable, trustworthy digital economy today relies on the intelligent and efficient operation of a multitude of software platforms and systems deployed at scale and in a distributed way, that bring the world together, help people connect, discover, interact, collaborate, learn, trade, transact, and share knowledge or content. Reliable, intelligent transport of digital information is the lifeblood of this economy. Securing the infrastructural underpinnings of this economy is increasingly recognized as being as critical as securing the pillars of the brick-and-mortar economies of old. The vast majority of these platforms and systems rely on networks to interconnect the sensors that bring data into the cloud for processing and enable data flow back out to the end-users. The growing number of IoT smart infrastructures are built to move beyond the traditional data collection role of legacy IoT systems, and automate the decision-making, control, and operation of physical systems (Chowdhury et al., 2022; Challoumis, 2025; Das & Adhikari, 2025).

Routine operation of these systems requires an ever-deepening trust and reliance on the seamless functioning of the infrastructure, 365 days a year, 24/7. In an era of information technology ubiquity, failures in service availability of even a few minutes can have catastrophic implications for business, society, and even national interest. While the physical infrastructure of these ICT systems has always been subject to wear-and-tear failures from equipment components failing or losing connectivity, the rapidly increasing connectivity demands for the flow of data from the surging number of things in the IoT, compounded by the increasingly complex network traffic dynamics would now be pushing operational reliability requirements from the core heart of the infrastructure to the edge. These components will also have to increasingly accommodate a load of control traffic originating from the AI/ML algorithms and models that drive intelligent operations of the smart infrastructures (Fadojutimi et al., n.d.; Jacob et al., 2021; Jana & Saha, 2021).

Connection counts are accelerating for a variety of IoT devices, with the enterprise sector among the leaders. IoT is used as a way to leverage and extend the business model value of existing products—for example, by enhancing products with features enabled by connectivity. Security continues to be a top concern across IoT verticals, while critical infrastructure, transportation systems, and smart cities are investing heavily (Somanathan, 2024; Ponnusamy & Aruldas, 2025).

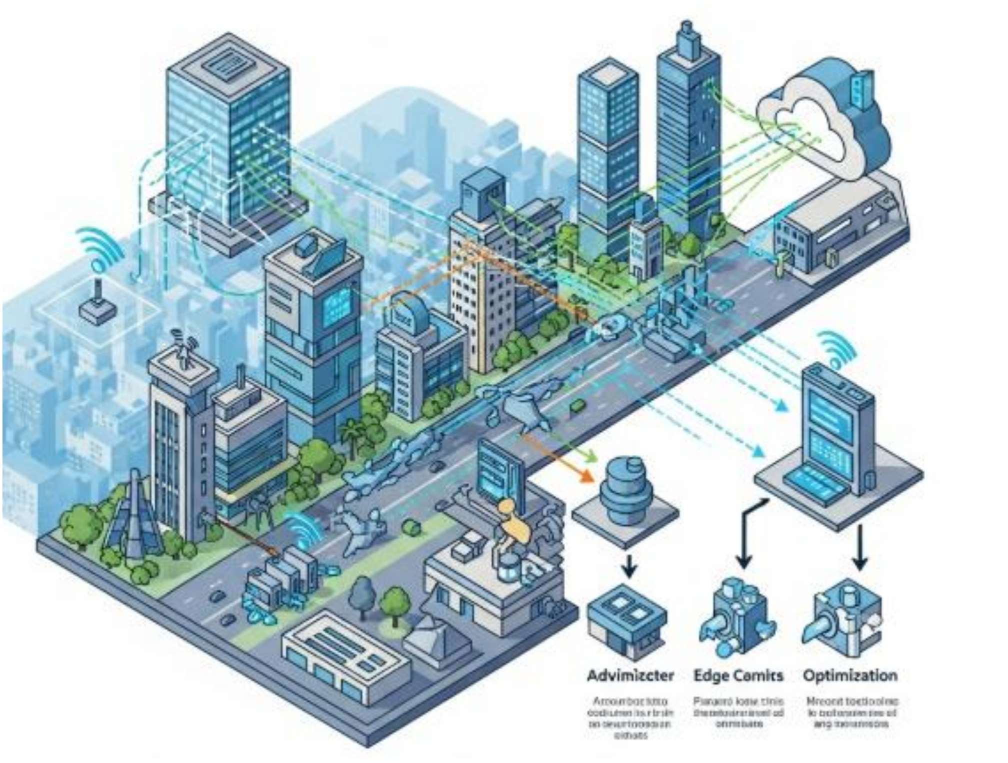

Fig 12.1: Future-Proofing Networks

12.2. Understanding the Current Landscape

As the importance of Artificial Intelligence, machine learning, Internet of Things devices, and smart infrastructure grows in the enterprise, economic, and consumer segments, questions come more and more with the influence of these technologies on the near and far future. Questions that lead businesses and governments to investigate the impact of these technologies so as to determine strategy and investment roadmaps. This chapter reviews the status of these technologies, with an eye on providing an overview of the technical landscape and insights regarding potential impacts on enterprise infrastructure.

At the highest level, AI-related technologies can be divided into data, algorithms, and infrastructure. Data: over 90% of data generated in the world today is considered unstructured. This data lies outside the capability of contemporary business intelligence systems. A growing number of vendors are providing improved tools for discovering patterns in unstructured data, tools that enable the creation of more engaging customer experiences while helping to identify opportunities for increased operational efficiency. Algorithms: popular AI technologies include natural language processing, speech recognition, virtual agents, intelligent search, sentiment and emotion analysis, video understanding, image recognition, machine learning modeling, and machine learning operations. Infrastructure: most investments are going into enabling infrastructure, which includes chips optimized to provide capability at all levels of the AI stack. Cloud companies offer chips as a way to gain differentiation while also enabling customers to get the best price-performance when deploying AI workloads.

12.2.1. Overview of AI Technologies

Artificial Intelligence (AI) can be defined as the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. More formally, it is an area of computer science that emphasizes the creation of intelligent machines that work and react like humans. Specific applications of AI include expert systems, speech recognition and machine vision. Devising systems that exhibit characteristics generally associated with intelligence, including the ability to learn, plan, solve problems, think abstractly, comprehend complex ideas, and learn from experience, has been a longstanding goal of AI development.

Artificial intelligence is requisite to all next-generation technologies that deploy large numbers of sensors with IoT infrastructures and require higher autonomy. Artificial intelligence comprises many subfields; areas that are still uncommon outside of research centers, but that have made important progress and that have decreased needed training in large networks for less specific applications. AI can be decomposed in Low-level AI: Lower-level algorithms for processing sensory input are an essential part of any AI system. These involve techniques for data processing and lower-level decision making, such as traditional machine learning for supervised and semi-supervised classification and pattern recognition, traditional optimization methods for particular problems and neural networks. Mid-level AI: The properties or references of a chatbot, for instance, are set in a mid-level. These algorithms focus on creating semi-plausible models of the world and for putting together coherent environments and storylines. These algorithms include language understanding: algorithms for domain-specific statistical parsing or for word embedding and latent semantic analysis methods. High-Level AI fielding a fast and human-like chatbot is mostly a high-level AI task. At this level one expects algorithms that are able to deal with what is commonly called common sense knowledge, which makes conversations (and most tasks) trivial or at least understandable to human beings.

12.2.2. The Rise of IoT Devices

The Internet of Things (IoT) encompasses the technologies that enable physical objects and devices to connect to the Internet. Examples include home automation devices, industrial control sensors, commercial property analysis devices, and traffic and transportation management sensors. The number of IoT devices in the world has exploded in recent years and new use cases for IoT devices seem to appear daily. IoT devices and sensors gather, send, and receive data. IoT devices are often inexpensive and small. Significantly, IoT devices often require very little power and often send their data in intermittent bursts, making them ideal for deployment in mass numbers. Networks are, therefore, increasingly connecting vast amounts of IoT technology to the Internet.

The sheer volume of IoT devices presents challenges for deployment and scaling. The scale of the user base places enormous stress on network resources, both on the packet volume transmitted and received by large data centers, as well as on the need for real-time reaction across massive geo-distributed IoT installations. The standardized high volume protocols for IoT devices are ideal for high-disillusionment density configurations. The implementation details of how endpoints and servers securely connect, how devices are identified and managed, and how real-time applications are deployed are all complicated and remain aspects of essential research that will define the future direction of IoT networking deployment.

12.2.3. Smart Infrastructure Trends

Infrastructure refers to the physical systems of a country, including transportation, communication, sewage, water, and electric systems. Current trends in smart infrastructure and key elements are represented in urbanization, advanced technologies, IoT everywhere, and data-driven governance are key drivers of the Smart Infrastructure ecosystem. After 150 years of industrialization, the world is entering an era of urbanization. By the middle of this century, it is predicted that 70 to 90 percent of the population will live in cities. This reality imposes enormous pressure on city planners to implement smart transportation, smart housing, smart public safety, and smart utilities. Advanced technologies are revolutionizing country infrastructure in many sectors. Industries are capitalizing on new advanced technologies to build trillion-dollar businesses that create jobs, consume massive amounts of raw materials, and improve living standards around the world. The combination of lighter, stronger materials, computer-aided design, nanotechnology, biotechnology, robotics, and 3D printing promise to radically change manufacturing. In addition, two developments presented by new information and communications technologies are the ability to connect effectively almost to every device and the extreme improvement in processing power, storing capacity, and data transmission. Infrastructure is key to economic, social, and cultural development. However, it is increasingly difficult to invest in infrastructure and provide social returns. The majority of these opportunities are found in developing countries, where a giant infrastructure investment gap exists and will persist for years.

12.3. Challenges in Network Infrastructure

Network infrastructure underpins the Internet and is rapidly evolving to have an increasing role, in both physical and social terms, as critical infrastructure that society relies on to function. Key issues in the deployment of the Internet infrastructure as a service along with the requirements for current and next generations of applications and services are highlighted. The increasing density of connected devices and the emergence of Bandwidth-on-Demand and utilities developed by new application contexts such as Internet of Things, Edge Computing and Artificial Intelligence augurs radical changes in the architecture of the Internet infrastructure in the near future. These changes are exacerbated by increased resource constraints arising predominantly due to the anticipated growth of traffic and behavioral changes. As a result, the elements of critical infrastructure associated with the Internet, which include data, fabrication plants, devices, networks, and services i.e. network infrastructure, are vulnerable to misuse such that due to malicious motivations of either external entities or internal actors, clients and users of such services are exposed to risk. This critical infrastructure, which is expected to be secure, resilient, scalable, and available for current and future users, is also being challenged by geopolitical pressures.

Accordingly, the Internet serves a diverse range of technologies, applications, and services which impose a combination of diverse, and at times conflicting, requirements on the critical infrastructure. Currently, Internet infrastructure is developed in an ad-hoc manner primarily driven by commercial interests. Along with demand for traditional services such as content delivery, new streams, primarily driven by streaming of time-critical bursts of the Metaverse, on-demand e-commerce, and global social interaction among others, are anticipated to radically change the traffic load patterns, and therefore the architecture of the underpinning infrastructure resources. Managing an ad-hoc mix of current and future streams such that both are optimized calls for a revisioning of the design and deployment of critical infrastructure for the Internet.

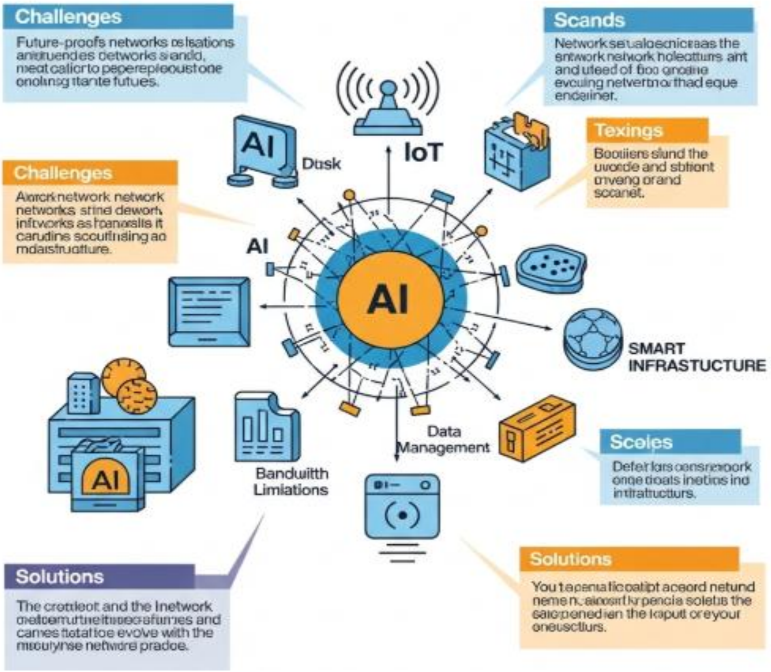
Challenges
Future-proofs networks relsations aniduendes detworks siandd, meatcalicrto peperepleoustone onolnsg ttante futues.
Scands
Networkseualoecnicraas the entwork network holeattums arit and uteed of foo qnoaine evculing netvertnorthad eque endeliner.
IoT
AI
Dusk
Texings
Booiiers slund the uvorde and sbtiont onveng orand scanet.
Challenges
Aorcrknetwork network networks stind dewort infworks as hoanoralls it carudins scoufindingao mdaisfruoture.
AI
AI
SMART INFRASTUCTURE
AI
Bandwiith Limiations
Data Management
Sceles
Defeirlarscensrenoork onde doals inetios ind intrattuctiurs.
Solutions
The crotdeot and the Inetwork oreltcemurtueituseeafumes and cames ftetatioe evolve with the mroulynse netwcre pradoe.
Solutions
You tapenta lioatipt acoord netund neme n.aioosrl krpencia soletts the saiepened ien the iapul oreyour oneuscturs.

Fig 12.2: Challenges in Network Infrastructure

12.3.1. Scalability Issues

The cornerstone for the deployment of AI and IoT at scale is the network infrastructure. Current global computer network infrastructures, including the Internet and Telco carrier backbones, represent the largest-scale, most critical platforms for service delivery to date. Yet, these complex systems have been built over decades via piecemeal upgrades to core technologies, pushing them into the realm of cobbled-together architectures that may be ill-prepared for the next round of abrupt paradigm shifts. As we ramp up to tens of billions of connected devices, deploying new classes of real-time applications and moving vast quantities of raw data to shared processing centers for analysis, we will need to scale existing infrastructure as never before.

We need to retrofit and reinforce these long-extant infrastructures to be able to handle the new scale and type of demands likely to be found in AI/ML and IoT workloads.

While network bandwidth has continued its long-term trend of geometrically increasing capacity per dollar of investment, the power consumption of network devices and the floorspace required to house them has grown, as have the costs of building and maintaining networks in construction and staff resources. With predicted IoT comms, sensor, and service management costs soaring into the trillions of dollars in the coming decade, these inflationary pressures can no longer be ignored. Current Internet and telecom architectures cannot easily absorb and efficiently relay the volumes of high-bandwidth, low-latency communication patterns that characterize the execution of AI workloads. Embedded AI services will require all of the intelligence, alternative technologies, and innovative solutions of next-gen communications networks. These must be as instrumented, self-aware, efficient, and evolutionary as the AI/ML systems that they serve.

12.3.2. Security Vulnerabilities

Security vulnerabilities of the infrastructure are mainly driven by the high number of connected devices and the abundant sensitive data that they will process. Despite the opinion of several experts, a cybersecurity crisis has not yet happened. There are three fundamental factors that will make this crisis a certainty in the next years: (a) major technological shortcomings in the infrastructures that will prevent their protection, (b) the excessive number of devices connected that might be utilized to perform coordinated attacks, and (c) the relative simplicity of cybersecurity attacks in these infrastructures, when compared to their defense because of the constraints imposed by real-time requirements.

Although the huge speeds that may be achieved in future networks will make the protection of data in motion feasible, the remaining steps of the data paths will still remain vulnerable for some time. Unfortunately, data processed in these vulnerable steps are those that contain the most sensitive information. Many data sources, in addition to consuming information, will also provide it, reversing the current paradigm of digital content consumption. Data consumption and provision will have to be based on trust. Actually, the only guarantee to achieve this trust is the payment, which in most cases will be done through cryptocurrencies or similar means. The resulting strong dependence on many devices, some of them IoT devices, to maintain the trust on the blockchain blocks that will record digital transactions and digital content sharing will be a serious threat for cybersecurity. The success of a blockchain attack will jeopardize the correct functioning of the decentralized services associated with the corresponding blockchain. On the contrary, the IoT cyberspace ecosystem will be relatively simple to defend because of the urgency of responding to critical situations. Cybersecurity capabilities will be merged with the intelligence functionalities required, creating a combined solution that will allow authenticating and relating multiple events in the time and space domains of the life cycle of the monitored processes.

12.3.3. Latency and Performance Bottlenecks

As the decade closes, Artificial Intelligence (AI)-related workloads are projected to account for two-thirds of all datacenter workloads and 75% of total assembly in semiconductor fabs. The AI boom does not happen in a void. It faces the same infrastructural challenges that existed before it. Barring the different developmental stages and scaling phenomenologies of this new generation of AI workloads, it is clear that the latency and performance profile of contemporary network systems is grossly unfavorable to the one that we will need in order to unleash AI's potential. There is an extreme and growing imbalance today between the throughput needed to get countless scores of CPU and GPU cycles moving per datacenter node per second exampling what is needed to assemble tomorrow's vast and growing neural nets on one hand, and the actual network and storage bandwidth available on the other. Cycles are going to waste, growing quietly hungry for data that are being rotated out to the colder edges of distributed storage systems.

Throughput, no doubt, is a powerful performance scaling die, especially as the cores widen. But it is beginning to reach its limits. The simple truth is that network and on-node storage latency grew comparably during the last very dense 45 years of Moore's Law, by a factor of 6× and 50× respectively. Each bit of access latency of the average microcontroller has grown from 200-1,000 cycles in 1971 to the desktop keyboard range of 1,000,000-15,000,000 cycles now, the result of unmitigated cycle stealing, equally monumentally on-chip cycle stealing capabilities, and architectural assumptions made 50 years ago that quickly bit the dust. Scale and increase in chip density alone cannot sustain and indeed are breaking the denormalization argument that deems network and on-chip memory latency unimportant for performance. Along with this, and for the same reasons, DRAM has lost its monopoly on what used to be a data persistence-only layer for desktop computing. It is being unduly stressed in embattled datacenters everywhere, as it becomes responsible for a major share of the total assembly.

12.4. Key Technologies for Future-Proofing

In order to make networks able to support the increasing requirements coming from new applications, service, and use cases, in this chapter we describe some of the enabling technologies that are playing an important role in future-proofing networks and allow the required degree of flexibility, agility, and programmability. In particular, we are looking at 5G and beyond systems, edge computing solutions –where the concept of edge is a source of confusion, given that it can refer to the C-RAN, to cloudlets and to Local Telco Factories–, Network Function Virtualization and Software-Defined Networking. These technologies do not have the same capabilities but, in many cases, are complementary to each other, and, when considered together, they may allow at the level of a complete network to provide the required level of flexibility, agility, performance, and efficiency in missions critical for networking applications. Connecting every device, towards a massive Internet of Things (IoT); providing a ubiquitous 10 Gbps service provisioning for everybody, everywhere, and at any time; guaranteeing ultra-reliable low latency communications services; offering resources immediately, in a flexible and on-demand way; being able to support verticals in specific networking applications, from industrial automation to eHealth and connected vehicles: these are some of the objectives within the so-called Fifth Generation (5G) of mobile communication platforms and system. Allowed by the availability of wide-band carrier frequencies in the mmWave, and the possibility of very dense deployments using digital small cells, the 5G vision goes well beyond that of the Fourth Generation and is opening the way for the communication network evolution that aims to comply with the very stringent performance indices and requirements needed by the next generation of vertical applications. It is therefore truly intertwined with the current enabling vision of Smart Infrastructures.

12.4.1. 5G and Beyond

5G offers enormous capabilities to meet these requirements and opens novel opportunities across multiple industries. It provides high data rate, ultra-reliable low-latency communication, and massive machine type communication. 5G comprises new radio frequency bands ranging from sub-1GHz to sub-100GHz, large channel bandwidths, dense deployment of cell infrastructure, and novel MIMO technologies. 5G leverages distributed edge computing to enable ultra-low tether latency by laying various distributed compute and storage resources close to the end devices. Network slicing enables massive scale, energy efficiency, and isolation between different use cases. Industry 4.0 and smart transportation, cities, and health are a few of the higher-layer use cases that can benefit from 5G capabilities.

The above capabilities have been motivated primarily by mobile broadband applications, with massive end-user video consumption being at the forefront. The tele-traffic growth and predictions around growth have been unprecedented, doubling mobile data traffic every 3 years and growing 40% over the past year alone. It is estimated that consumer mobile data traffic will reach 77EB at a CAGR of 46%, accounting for 95% of total mobile traffic, in six years. In contrast, the requirements for AI, IoT, and smart infrastructure use cases, especially for latency, reliability, scale, and energy efficiency, have been largely unaddressed in the current mobile broadband era. Although 5G will not solve all problems and the introduced capabilities may not be enough, it is a stepping stone to address these issues and prepare mobile networks for new use cases.

12.4.2. Edge Computing Solutions

Foreseeing a future composed of millions of connected devices, the need to have low latency access to data has forced developers to think up new architectures that move compute resources from centralized data center locations to the edge of the network. Internet of Things devices, Artificial Intelligence services, and Smart Infrastructure systems are born at the edge, and logic needs to run as close as possible to them. The use of edge compute nodes moves the data processing load closer to the origin of the data, thus improving latency and network utilization.

Edge cloud platforms are designed around the concept of hosting cloud-like applications at the edge of the network. They deliver the same technology stacks available in centralized clouds and software environments but deploy those stacks and services at the local scale of edge sites. This deployment model opens many possibilities for application architecture, management, and scalability, and introduces new options for transforming the way software intelligence is applied in nearly any business or organization.

At the edge, data is acquired and generally processed in real time. This accelerates many tasks that would require waiting for a connection to a centralized cloud to be completed. Limiting the encryption-decryption-processing cycle to smaller stacks by edge hosting logic solves latency problems in many use cases. Moreover, it is also possible to maintain a continuous operations window, as local compute nodes continue processing and pushing data packets, even when they are offline. Centralized resources are in charge of collecting processed data and preparing algorithms when the connection to the central site is up, thus ensuring continuity.

12.4.3. Network Function Virtualization (NFV)

Network Function Virtualization (NFV) is adjacent but not the same as Cloud-Radio Access Network (C-RAN) technology; whilst C-RAN segments and virtualizes radio components of radio access networks, NFV provides a more generic use of cloud technology to host all network functions in virtual containers, placed strategically in the network, using the broader infrastructure that technology provides. NFV offers support for Edge Networks and for Deployment of Low Latency Applications and Services. Virtualized Edge Solutions Lower Latency Requirements for Multiple Concurrent Applications. Network Bottlenecks Stemming from Hardwired Infrastructure Would Be

Addressed by NFV. NFV Decouples Network Hardwired Technology from Device Functionality Offered. Different Services, When Activated Require Different Functions, A Softwarization of the Hardwired Device Network Technology and Functionality Mapping Would Be Required. NFV Is the Tool for Enabling That Softwarization of the Devices.

Network Function Virtualization (NFV) is a technology that has been defined to address the decoupling of network functions from the devices they are mapped to. The Initial Impulse Came from the Growing Complexity of Network Services. A True Need for Implementing Optimization in All Network Services, from Customer at the Edge to the Access Network, the Transport, and the Core Network Impulse the Provisioning and Activation Plans Needed, with an Increase in Network Opex and Capex Requirements, Incentivizing All Major Operators to Consider Ways of Increasing Efficiency with the Implementation of Software Technology. Due to the Increasing Demand of Mobile Data Transmission, A Need for Investing with an Increase in Network Capex and Opex Requirements Stemming from the Investment in Optimization of Network Services, from the Device at the Edge to the Core Network Could Be Addressed through the Use of an NFV Approach that Could Allow for Low-cost Implementation and Deployment of Network Solutions in the Various Network Components.

12.4.4. Software-Defined Networking (SDN)

Software-defined networking (SDN) is an emerging approach to the design and management of networks that decouples the network control from the data forwarding elements. This approach has matured into a number of multipurpose programmable platforms. By relying on increased programmability of the data forwarding elements and abstracting the network control and management resources, SDN enables global and in-depth network monitoring and control for many different applications. This transforms the function of networking equipment from closed boxes to open programmable platforms that can execute different services.

SDN also calculates and manages traffic flows through the network in its control software, based on global knowledge of the network and the services provided. It builds a flow table that lays out every path through the network for every flow and populates the flow tables in the switches along each path. Then, it watches for flow table misses to detect new flows. When switches receive packets of a new flow and recognize that they are not listed in the flow table, they send the packets to the controller, which then executes a flow table miss routine using its own logic as needed and updates the flow tables to direct the packets of the new flow to their destinations and to deliver them to the right switches in the meantime. SDN provides a programmatic interface for adding new network transfers through its routing or forwarding mechanisms, enabling application developers to create new applications and overlay services layered on top of the basic packet-forwarding infrastructure there. It allows the flow routing to be adaptive and optimized.

12.5. Design Principles for Modern Networks

Networks, both wired and wireless, have become critical enablers for all types of object-to-object and person-to-object interaction, driven by both the IoT and various AI techniques. Connectivity is a key foundation to support seamless AI, IoT, and smart infrastructure interactions, which are necessary to deliver new features and capabilities, provide a better user experience, and harness the new dynamics of the digital transformation of our society and its economy. Connectivity, in this sense, involves the transfer of different modalities of data at different levels of performance to cloud or edge AI-based computing resources and services, sometimes with deterministic performance requirements. Apart from artificial intelligence, modern networks face demands evolving from the need to enable the internet of things, which includes the provisioning of connectivity for a massive number of machines in a heterogeneous manner, in the case of industrial automation, asset monitoring, and production optimization, as well as the support for new data-driven smart infrastructures and smart cities, whose development rely on improved efficiency, productivity, and optimization of services.

From our perspective, the infrastructure to deliver the new types of interactions supported by AI and enhanced by IoT involves a combination of wide area networks, such as the internet, cellular networks and satellite, with local area networks, such as fixed and radio access technologies. From here, we derive the challenges we highlight in this manifesto. They cut across multiple layers of the communication stack, from the physical layer to functionality-enabled layers that support services, and range from device-centric, to connectivity-centric to data-centric challenges. To tackle these challenges, we advocate specific design principles for future-proofing networks for AI IoT and smart infrastructure. These design principles are modular and flexible capabilities, interoperability standards, and automation and orchestration functionalities.

12.5.1. Modularity and Flexibility

To effectively support the service requirements of next-generation AI-ML, IoT, and smart infrastructure and help carve out a business model with the BAT-rich intelligent digital services, networks need to be designed with certain basic principles in mind. In the following sections, we will first present what we propose as some design principles for modern networks. We will then delve into the details of each design principle by drawing on recent technology advances within and also outside of the telecommunications industry such as the hardware architecture used in data centers for large scale machine learning and distributed systems, AI CPUs, distributed ledgers and other smart infrastructures, Open RAN, advanced remote control capability for operations support, microsegmentation, CI/CD DevOps, advanced visualization tools and AR, and others. Last, we will translate the desired design principles into tangible, concrete steps that are actionable by network service providers to ensure their networks are aligned to meeting these next-generation relative service demands.

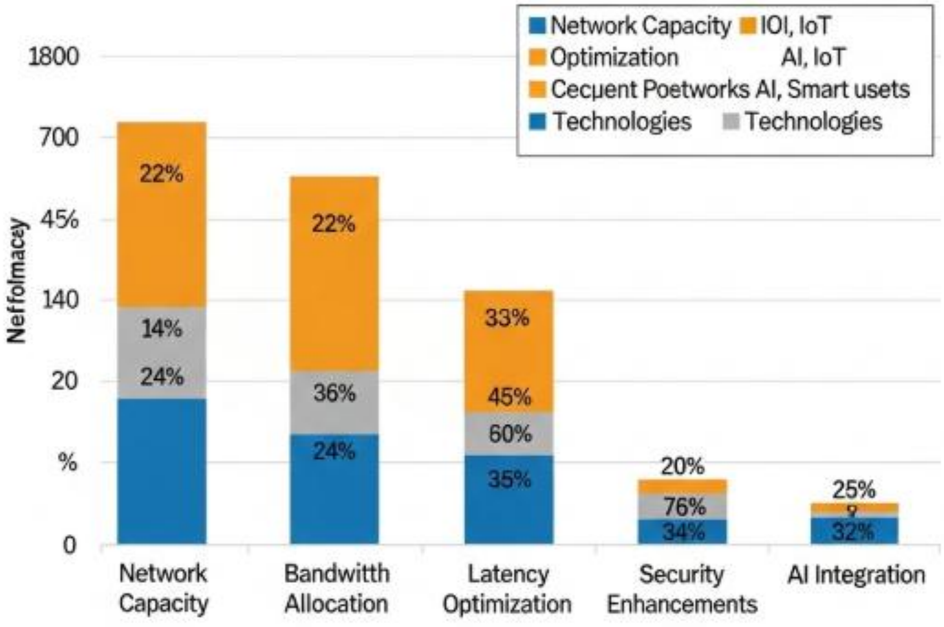

Fig 12.3: Future-Proofing Networks for AI, IoT, and Smart Infrastructure

The first design principle of modern networks is modularity and flexibility. Next-generation networks will need to deliver a diverse set of services that carry different capabilities and service characteristics such as the service latency, traffic prediction, and network resource affinity. In particular, the rapid proliferation and adoption of AI applications and IoT devices often gives rise to very bursty behavior such as very aggressive traffic spikes. This necessitates sophisticated network design techniques that help tailor the network to adequately support such service characteristics. For example, certain network designs may be able to achieve ultra-low latency under offered loads lower than 50% of average network traffic loads, while still other network resource layouts can help minimize the probability of severe congestion arising by having additional resources when the network resource utilization is greater than 80%.

12.5.2. Interoperability Standards

Although modularity allows organizations to treat their networks as composed of interconnected parts, the next critical question is: How does one ensure that any piece of hardware or software from different vendors can, in fact, work together? This is where interoperability standards come into play. These standards define how every piece involved in a network operates so that other pieces know how to interact smoothly. For decades, such standardization allowed computers, routers, web servers, and other components from disparate vendors to work together, enabling the rapid growth of both the Internet and enterprise networks. Recently, however, a new type of company has begun to emerge: one that has powerful end-to-end control of its entire infrastructure and stack—an ecosystem approach.

In recent years, many large cloud providers, network vendors, and enterprise IT departments have pursued the opposite strategy of targeting the entire piece of software or hardware service model through end-to-end control over their network architecture but with the promise of simplicity and out-of-the-box functionality. Such solutions, however, often rely on specialized hardware products. This undermines common interoperability standards for the physical and data link layers. Nevertheless, it serves as a reminder of how increasingly complex systems can risk greater complexity, vendor lock-in, and worse functionality. Effective counter strategies can be shaped through standards to ensure wide interoperability and innovation.

12.5.3. Automation and Orchestration

As systems become larger and more complex, automation will become a necessity. While automation isn't new in networking, it has traditionally been focused on the minor task of configuration management. Continuing the trend of general purpose programmability, we believe the real goal of automation should be to minimize human intervention as technology stacks become more diverse, as well as completely opaque. More than configuration management, the automation focus should be on performance management, fault management, and security management. Only through fundamental task automation can we possibly hope to stay in touch with what is going at the application level. The most dramatic example of network task automation can be seen in resource management; these clouds are unbelievably massive, and yet are maintained with a tiny number of programmers.

As a community, we have developed an elegant solution to the automation problem in the virtual machine code and its associated language bindings. Virtual machines provide us a way to write significantly simpler code to control performing machines, making our data centers easier to manage, among other things. I believe we haven’t really seen virtual machines become part of the networking stack. Network devices such as routers and switches do not have a resource abstraction. What this means is that network virtualization is usually left to the orchestrator. Orchestrators are limited in what they can do, because there are never enough virtualization or automation tools if routing etc. is not part of the abstraction.

So, this is where our future resides: the communication stack will have to expose a set of resource abstractions to allow greater flexibility in path management. Imagine that those path resources are truly managed within a resource manager, allowing for the higher level orchestrators to truly become plug and play, allowing researchers to define new resource management techniques and publish them for others to use.

12.6. Case Studies of Successful Implementations

The previous sections have set the groundwork to support the use of networks with AI, IoT, and smart infrastructure applications. However, in proposed research and applications, there is still much work to be done before deploying the foundational and supporting technologies at a massive scale. Due to the growing applicability of AI in domains ranging from healthcare to intelligent transport systems, there is a growing interest in the deployment of smart infrastructure that is intertwined with the use of networks. This future direction for the networks is what we will cross-examine in this section by presenting some examples of successfully implemented systems that utilize these essential concepts.

Current available smart infrastructure is being incrementally designed to cater to the communication demands with the use of the latest AI and IoT technologies. In this section, we note widely used use cases that showcase the employment of networks with an intelligent footprint. Then we analyze the enabling technologies and the challenges behind the development of each of these representative use cases. The goal of this discussion is to present available evidence showing successful cases of using these technologies that build up assurance and trust in smart infrastructure, which are the thematic ideas of this chapter and the book overall. This section lays the foundation to highlight, in the next chapters, the foundational technologies that are required and need to be further developed for the use of future networks. Lastly, by providing evidence of the impact of these technologies currently, we hope to assist the academic community and other stakeholders to prepare convincing arguments that can support the future use of a future generation of wireless networks with a built-in intelligent footprint.

12.6.1. AI-Driven Network Management

Managing networks efficiently and effectively is no small task, but it is essential as we connect devices in the thousands, rushing towards 100 billion connected devices. Technologies such as IoT and AI accelerate the networking acceleration, and it is becoming impossible for humans to manage the networks with increasing complexity. We have to look for help from intelligent solutions to manage and optimize networks in an autonomous fashion. In this context, AI is the one area where we can look for solutions due to its predictive and explanatory nature. Coupled with other statistical advancements in the field of reinforcement learning paired with affordable computing and increased data sharing, we can design systems that can turn the handling of huge networking complexity into a relatively easy and controlled optimization solution. We help enable both problems and solutions here under this section. The first step is to create datasets for autonomous learning. The second part is to create machine learning models that can learn from big data and create patterns from the data and generate models that can take away human guessing. The final piece of the AI control loop is closed loop control which uses AI at regular short time intervals during the day and makes near real time events to automate the human intervention in managing networks. The assembled engineering experts at the right time from engineering experts with cloud, virtualization, IoT, and AI/ML skills.

Through this essay, we hope to present collages of knowledge and solutions to inspire future researchers and industry practitioners to address these areas in investigating the remaining control pieces belonging to the embedded networking systems for numerous applications in both the consumer and enterprise segments. Specifically, the knowledge represents concrete application examples in enabling low power wide area networking for industry use cases.

12.6.2. IoT-Enabled Smart Cities

Urban spaces face challenges such as overpopulation, increasing carbon footprint levels, infrastructure decay, lack of security and safety, transport inefficiencies, and the ineffectiveness of healthcare and other services delivery. Smart cities can address these issues, leveraging IoT, Artificial Intelligence, Big Data, etc. IoT solutions increase citizen engagement and improve service delivery and more efficient use of resources in urban areas. For example, with smart waste management solutions, cities and businesses can optimize waste collection service routes and schedules through real-time waste level tracking, reducing costs, carbon emissions, and traffic congestion while increasing service reliability. Road monitoring systems facilitate communication with city traffic controllers and transportation agencies by transmitting congestion data and incident data, enabling timely traffic condition assessment and control.

Smart cities also improve sustainability through road health monitoring, intelligent water management, and energy network management. Moreover, smart surveillance monitoring cameras prevent theft, violent criminal behavior, and other security violations such as vandalism. Real-time monitoring detection capabilities are very effective for manual surveillance, allowing fast responses during extreme situations. Automated security violations sensory detection systems are also widely used in smart cities, triggering alarms to notify authorities of any alarming situations.

12.6.3. Resilient Smart Grids

To create the smart grids of the future will require the integration of many different elements, one of these being telecommunications networks with Artificial Intelligence at the core. With Artificial Intelligence, smart grids can do more than just management of the infrastructure, they can assist human experts to make better, faster allocation of assets, repair of outages, and upgrading of resources when necessary. Humans will always need to be involved for the bulk of smart grid management, but I can make that management much more effective through global awareness of other systems dependencies on the smart grid. Until now, the two systems have been kept separate in order not to allow cross-contamination of assets. As the dialogue gets deeper, the results will facilitate decision making, optimize maintenance, and resolution times. Smart grid networks have been a target for cyber-attacks, most especially during military conflict, as a way to degrade public services. Many experiments have validated that telecommunications networks are susceptible to denial of service attacks which can impede the service of the electric grid and further cause widespread public service outage.

As the response time is very low, consideration must be made to have backup connections so that the detection surveillance network is capable of maintaining the reaction during the scheduled maintenance of the telecommunication networks used to detect these services. A possible implementation can be based on multi-vendor product and multi-domain fabrication in order to automate the rerouting to ensure the resilient behavior. Trust and dependency are two categories expressing the level of collaboration among the key parties in both the Smart Grid and the Telecommunications Networks domains. Circular dependencies with other cycles that include the Smart Grid and the Telecommunications Domain can hinder resiliency, sustainability, and increase risk. These circular dependencies need to be investigated and managed throughout the entire lifecycle for a successful implementation.

12.7. Conclusion

Progress in artificial intelligence (AI), including machine learning (ML) and deep learning (DL) capabilities, has largely been delivered over previous decades by advances in the capacity and performance of general-purpose processors. Nowadays, the compute demands of many AI applications are being supported by dedicated hardware accelerators, typically termed AI accelerators, such as deep neural network accelerators and graphics processing units (GPUs). There has been great interest in hardware accelerators for the inference phase of the machine learning pipeline, but also increasingly for the training phase as well, including the continued exploration of alternative architectures and techniques. Likewise, the deployment of massive foundational NLP models and image audio models is placing greater demand for high-performance processing and storage. The trend in many AI applications is to increase speed and efficiency, and lower-cost deployment.

More advanced AI, IoT, and smart infrastructure applications are rapidly developing momentum in the mainstream, delivering transformational benefits to tools, products, and systems of great value to society. Examples across the consumer/small business, enterprise, and societal segments include AR/VR immersive experiences, distributed collaborative workspaces, mobile-assisted retail experiences, collaborative robots in unmanned shops, industry systems of intelligent asset management, digital twins of urban infrastructure, autonomous vehicles, and smart border systems of remote monitoring and control to deter illegal immigration and cross-border smuggling. Driven by exciting innovations in such diverse areas as ultra-low component-cost sensors with ever-better sensitivity and accuracy levels, hyper-scaled wireless, IoT, and data center cloud infrastructure, and fast-evolving machine learning algorithms for wide industry datasets, these applications and use cases now also benefit from vibrant open ecosystem collaborations to a very high degree.

12.7.1. Future Trends

In the coming years, two pillars will be required for a future-proof infrastructure: soil infrastructures and smart networks, both of them focused on the automation, management and orchestration, synchronization, and standard satellite connectivity that AI, Internet of Things, and Smart Infrastructures need all around the planet. Data and the capacity to process it in real-time, turning it into knowledge, is the real enabler of the future. The smart infrastructure reacts with control of the different assets; these assets generate data that is transported to the Data Centers via Cloud Networking technologies for their early processing and finally acted upon by the smart infrastructure. The movement Store-Process-Act is the key. This movement is mainly focused on Store, positioning very close and fast the satellite connectivity to the infrastructure established in its first stages and finally moving the AI engines close to the edge. The propulsion of the robots will come from the satellites positioned in non-geostationary orbits that will transport data and intelligence back and forth to the geo orbital and terrestrial Data Centers. Cyber-resilience will be the final feature of the future Life 4.0 by point-to-point connectivity that avoids all the possible maneuvers to mitigate risks and prolong the uncertainty in the middle of the Data routing between the edge and the Cloud. Cyber-resilience will also cover the small terrestrial communications that will be empowered in capacity and ultra-low latency by Low Altitude Access and Satellite Constellations.

References

Das, A., & Adhikari, N. (2025). Future-Proofing IoT Security: The Impact of Artificial Intelligence. In The Intersection of 6G, AI/Machine Learning, and Embedded Systems (pp. 369-390). CRC Press.

Ponnusamy, V., & Aruldas, H. R. (2025). Future-Proofing Emerging Technologies. In Future-Proofing Emerging Technologies for Business Transformation (pp. 439-474). IGI Global Scientific Publishing.

Somanathan, S. (2024). Future-Proofing Project Management with AI and Blockchain: Trends, Challenges, and Opportunities. Nanotechnology Perceptions (ISSN: 1660-6795), 20, S8.

Jacob, I., Lawson, R., & Smith, R. (2021). Future-Proofing AI and Cloud Systems: The Intersection of Quantum and Cybersecurity.

Chowdhury, S., Zhu, J., & Center, T. I. D. (2022). Future-proof transportation infrastructure through proactive, intelligent, and public-involved planning and management.

Challoumis, C. (2025). Future-Proofing Your Investment Strategy: Embracing AI And Data Analytics.

Jana, A. K., & Saha, S. (2021). AI-Powered Network Packet Switching-A Wa y Forward for Future-Ready Communication Systems. Europea n Journal of Advances in Engineering and Technology, 8, 37-41.

Fadojutimi, B., Israel, A., Arowosegbe, O. B., & Ashi, T. A. FUTURE-PROOFING SUPPLY CHAINS: LEVERAGING ERP PLATFORMS FOR ADVANCED AUTOMATION AND INTEROPERABILITY.