Journal of Artificial Intelligence Practice (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/jaip.2024.070103
ISSN 2371-8412 Vol. 7 Num. 1

Application of Artificial Intelligence in Computer Network Technology in the Age of Big Data

Yang Zhenpeng

Department of Literature and Law, Hongshan College of Nanjing University of Finance and Economics, Nanjing, Jiangsu, 210003, China
17853893449m@sina.cn

Keywords: Big Data Era, Artificial Intelligence, Computer Network Technology, Applied Research

Abstract: In the surging tides of big data, the symbiosis of artificial intelligence with computer networking has given birth to a plethora of innovations. An immense volume of data courses through the networks, serving as the novel fuel propelling society forward. Computer networking technology, as a crucial cornerstone for the transmission and processing of information in modern society, is undergoing monumental transformations. Big data ushers in unprecedented challenges and opportunities for network architecture, protocols, and even security measures. Concurrently, the swift advancement of artificial intelligence technologies further amplifies this phenomenon: every facet of network security, management, and data analysis is beginning to harness the efficiency and intelligent solutions offered by artificial intelligence. This synergy is driving networking technology beyond traditional boundaries, forging ahead into a future that promises greater intelligence and efficiency.

1. Introduction

In an era marked by a phenomenal surge in global data volumes, the term "big data" has transcended its origins in academia and permeated the public consciousness, expanding its definition beyond a mere collection of datasets to embody a complex fusion of technology, social dynamics, and, indeed, a directive in policy-making. Similarly, "artificial intelligence" has metamorphosed from a concept enshrined in science fiction to become the pivotal force propelling the advancement of contemporary technologies. Within this context, the interaction between these entities is no longer unidirectional but has evolved into an intricate and symbiotic relationship. As computer networking technology serves as the lifeblood intersecting all societal strata, its operation and evolution in this data-intensive age are urgently compelled to harness artificial intelligence in assuming pivotal roles. This integration is mandatory to augment efficiency, fortify security, and to confront the myriad challenges presented. Under this new paradigm, the application of artificial intelligence within the realm of computer networking stands as both a technical conundrum and a critical determinant poised to revolutionize occupational and domestic life.

2. Characteristics of the Big Data Era

In the deluge of the information age, individuals have gradually recognized that data is emerging as the novel engine propelling societal metamorphosis and technological innovation, ushered in by the advent of the 'Big Data' era. The era of Big Data is characterized by the voluminous troves of data engendered through the internet, Internet of Things, and an expanding array of smart devices, posing challenges and exerting forceful impacts upon conventional methodologies of data handling, while simultaneously presenting myriad industries with the prospect of transformative advancements. Within the context of this epoch, the explosive growth in data volumes stands as the most prominent hallmark. Every second, innumerable individuals and machines produce vast quantities of data—ranging from the text, images, and videos of social media to the recordings of commercial transactions, sensor readings from IoT devices, and comprehensive datasets of medical imaging. The information concealed within has vaulted from terabytes (TB) to petabytes (PB) and even exabytes (EB). The diversity of data types is similarly burgeoning, presenting in variegated formats and intricate structures. Traditional structured data, like database tables, no longer suffice to meet all dem, with unstructured data types such as text, images, and videos, and semi-structured content like emails and log files, comprising the heterogeneity of Big Data. The behavioral data of individuals and operational data of machines are also encompassed for consideration. With the surge in both data volume and variety comes an accelerated demand for data processing speeds. Enterprises and organizations yearn to analyze these vast datasets in real-time to make swift decisions in response to market fluctuations, thus imposing elevated demands on data processing technologies. For instance, the burgeoning realm of real-time data processing and stream computation serves to address this quest for velocity. Perhaps the most exhilarating shift lies in the ascension and excavation of data's intrinsic value. Within each set of data resides latent value awaiting discovery. Enterprises and research institutions are harnessing the powers of data mining, machine learning, and artificial intelligence to identify patterns, predict trends, and devise strategies from colossal datasets. For example, e-commerce platforms can tailor more personalized product recommendations by analyzing user behavior data; physicians can diagnose diseases with greater precision through the analysis of patient health records. Yet, this promising new field is not without its challenges. Data security and the safeguarding of privacy have become widely discussed concerns. Questions about how to mine data for its worth while protecting individual privacy, and how to prevent information breaches while capitalizing on the conveniences offered by data utilization, are issues that industry experts, academics, and policymakers must collectively address [1].

3. Artificial Intelligence in Computer Networks

3.1. Network Security

Cybersecurity encompasses a comprehensive concept employing technological and managerial strategies to shield network systems from unauthorized access, assaults, degradation, and other prospective hazards. Its fundamental tenets aim not only to safeguard the integrity and availability of data but also to ensure the confidentiality of information, thus preventing the disclosure of sensitive details. Within this perpetually developing and evolving digital realm, artificial intelligence has emerged as an indispensable force in the realm of cybersecurity. As a diligent and precise sentinel in the domain of cybersecurity, AI technologies apply machine learning algorithms to automatically assimilate and adjust to the increasing complexity of security threats and defensive measures. Amidst the vast torrents of data, artificial intelligence indefatigably analyzes log files, monitors anomalous behavior, and even anticipates trends in threats. When juxtaposed with

traditional security methods, AI can identify and respond to nascent malware and zero-day vulnerabilities more rapidly. In the bustling nexus of internet interactions, myriad security pitfalls lay hidden. As hackers constantly refine their tactics, AI continually evolves to meet these challenges. For instance, AI, through the prowess of deep learning, can discern subtle patterns within a multitude of phishing emails, thereby filtering them out and sheltering users from deception. Intelligent systems build upon their existing knowledge to ceaselessly refine themselves, thereby erecting an increasingly impregnable digital fortress. Furthermore, the integration of AI into cybersecurity solutions enables more sophisticated access control. By studying user behavior patterns, intelligent technology can react more swiftly to potential internal threats. It recognizes the typical activities of specific users and, upon detecting anomalous activities such as the misuse of user credentials, immediately issues alerts and restricts improper access to sensitive data and critical infrastructure. In the tangible world, the cybersecurity practices of financial institutions provide an instructive exemplar. In recent years, several banks have begun deploying AI-powered security systems to combat financial fraud. These systems, continuously learning from an array of transactional data, can instantaneously identify transactions that deviate from a client's usual pattern and promptly intercept potential fraudulent actions, thus safeguarding clients' financial assets [2].

3.2. Network Management and Optimization

Within the expansive cosmos of the internet, network administration and optimization function akin to an astute navigator, ensuring the rapid and efficient flow of information. These systems constantly uphold network stability and peak performance through vigilant monitoring of network conditions, scrutinizing data traffic, and adjusting resource distribution. With the swift evolution of artificial intelligence, it has insidiously infiltrated all facets of network management and optimization. Confronted with the enduring challenge of network congestion, the application of AI has demonstrated exceptional intelligence. Employing technologies such as deep learning, AI systems are capable of discerning traffic patterns amid the complexities of network data, much like discerning the melody in a confounding symphony. They not only predict peak usage times but also swiftly identify anomalous traffic, acting as vigilant guardians who preemptively signal alarms to avert potential hazards. Artificial intelligence has made notable strides in network resource allocation, optimizing bandwidth utilization in real-time and executing data routing with precision to ensure that resources are apportioned among users as needed. Thereby, each data packet is guided along the most efficient route, akin to forging a private thoroughfare through the vast digital realm. For instance, when AI detects a surge in demand for video conferencing, it promptly allocates additional bandwidth, constructing a capacious bridge of information to facilitate uninterrupted communication and ensure the smooth conduct of pivotal meetings. Furthermore, AI excels in perpetual learning and self-optimization, thereby evolving the intelligence of network management. After amassing a sufficient historical dataset, AI can more accurately forecast future network needs, dynamically adjusting network strategies to accommodate fluctuating loads and avoid resource waste. Such a network management system sharpens its wisdom through continuous learning, prediction, and adjustment, much like an experienced strategist maximizing the efficient utilization of network resources. Nonetheless, technological advancements never occur in isolation. As AI refines network optimization, considerations of privacy and security become paramount. Every advancement should be grounded in a profound understanding and careful assessment of data sensitivity and potential network vulnerabilities. Hence, the implementation of technology is accompanied by ongoing exploration and deep contemplation of possible ethical and security issues, ensuring intelligent optimization proceeds hand-in-hand with the stability and security of the future network environment [3].

3.3. Network Data Analytics

Network data analytics is a sophisticated practice that delves into the ocean of digital information, harnessing waves of collected data through intricate processes of curation and analysis to uncover intricate patterns, trends, and anomalies characteristic of online behavior. It acts as a luminary beacon penetrating the deep-sea darkness, illuminating not only the pathways of data flux but also delineating the profound architectural intricacies of the cyber realm. Augmented by the formidable prowess of artificial intelligence, network data analytics is rendered increasingly sagacious and efficacious. Machine learning algorithms are meticulously trained across diverse datasets and possess the intrinsic capacity to self-optimize, honing their proficiency in recognizing and adapting to the dynamic fluxes of the network milieu. When dispatched to the nexus of the network, these algorithms are adept at ensnaring the minutiae within the live currents of data, sifting through the cacophony to isolate signals that are quintessential for the fortitude of network security and performance. This intellectually automated interpretation not only is instrumental in preserving the well-being of the network infrastructure but also safeguards the seamless experience of the user constituency. As time proceeds, with relentless streams of data coursing from an array of sensors and log entries, the tools of network data analytics metaphorically mirror seasoned mariners steering the vessel of algorithms with steadfast precision. They have evolved intricate charts and tools for visualization that render the once nebulous data flows eminently discernible, offering network stewards a detailed tapestry of the operational state of affairs. Adding a touch of the arcane, the integration of deep learning techniques has propelled network data analytics beyond mere retrospective and real-time descriptions, grafting onto it the prescience of foresight. Parsing through historical data and identifying incipient causations, it is primed to signal impending congestions, malevolent intrusions, or other aberrations [4].

3.4. Cloud & Edge Computing

Amidst the surging tides of artificial intelligence, cloud computing and edge computing have birthed a novel paradigm of collaboration. Cloud computing is tasked with the provision of centralized data processing and storage solutions, while edge computing, by virtue of its proximity to the data source, executes instantaneous data processing capabilities with the intention of diminishing latency and conserving network bandwidth utilization. When one deliberates upon their application in the empirical realm, this synergy might well be deemed the progenitor of myriad innovative and efficient methodologies. Envision a quintessential scenario within the confines of a sensor-laden smart city, where voluminous data is perpetually spawned, from streetlight signals to surveillance cameras. In such milieu, to process and analyze these copious volumes of immediate data, the transmission of all intelligence back to a remote data center would evidently occasion immense latency and consume considerable bandwidth resources. Ergo, edge computing comes to the fore, adept at processing information on-site at the edge nodes where data is generated. For instance, an intelligent device affixed to a traffic signal can manipulate the changes of the light in real time to alleviate vehicular congestion. In essence, certain decisions that necessitate swift responses may thus be resolved just a step removed from the data source, thereby sensitively attuning to and responding to the subtle fluctuations of the city's pulse. Concurrently, cloud computing assumes a vital role. By conducting profound analyses on a vast compendium of processed data relayed from edge devices, it extracts and learns the longitudinal trends and patterns of the intelligent city. This stratified approach to analysis effectively distributes the load between real-time and non-real-time processing, optimizes the utilization of network resources, and concurrently maximizes the value derived from the data. Such applications demonstrate the staggering potential unleashed by the collaboration between cloud and edge computing. One can

eagerly envisage that, with the incessant evolution and refinement of technology, and with the aid of artificial intelligence, this cooperative endeavor holds great promise in molding an even more intelligent and interconnected world [5].

4. Big Data and Artificial Intelligence Synergy

4.1. Data-Driven Network Decision Making

Data-driven network decision-making pertains to the technique of harnessing vast quantities of data harvested from the network to guide and enhance the operational and administrative aspects of the network. Within this paradigm, artificial intelligence not only accrues data but also dissects it, uncovering patterns and trends, thereby astutely predicting and modulating network behaviors to achieve optimal performance. The data streams coalescing within the network are analogous to the life-blood coursing through veins, bearing the vitality and intellect of the entire network ecosystem. Data-driven network decisions are akin to a seasoned internist who, by interpreting the esoteric information within the blood, diagnoses and fine-tunes treatment plans. Artificial intelligence, serving as this physician's adept assistant, embarks on this process by persistently capturing information from an array of devices and interfaces—this information encompasses traffic data, application performance, user conduct, and even network security incidents. Once these data are amassed, they are funneled to a big data analytics platform, pervaded with an air of machine learning algorithms reminiscent of alchemists meticulously distilling valuable insights from the erstwhile chaotic data. The algorithmic probes delve into the data's core, learning and sculpting models, progressively enhancing their capacity to prognosticate forthcoming events. With the continuous refinement of these models, predicated on historical and real-time data analysis, artificial intelligence begins to adjudicate autonomously, absent any human oversight. For instance, in traffic congestion prediction, it can estimate when and where a link is likely to be overwhelmed by demand, and autonomously orchestrate the traffic prior to the eventuality. As a physician foresees illness and adopts preventative measures, so does artificial intelligence preemptively weave a safety net ahead of network exigencies, mitigating or obliterating the risk of potential system outages. It is imperative to also note that, throughout this process, network security remains an indispensable element. The artificial intelligence's aptitude for detecting atypical data flows and latent threats mirrors a nocturnal creature's night vision, capable of timely identifying and isolating malevolent attacks amidst the undercurrents, thereby ensuring the overall security and stability of the network [6].

4.2. Adaptive Learning and Predictive Modeling

Amidst the pervasive integration of artificial intelligence in today's milieu, adaptive learning and predictive modeling have emerged as cornerstones in the sophisticated evolution of computer networks. Such models, by harvesting data in real time and utilizing algorithms to incessantly fine-tune their parameters, acclimate to the ever-shifting network milieu, thereby furnishing precise predictions. Immersed in an ocean of data, adaptive learning and predictive models resemble an indefatigable scholar, tirelessly sifting through the data stream in pursuit of patterns, learning, and adapting, thus endowing the network with heightened intelligence. With their capacity for self-iteration, they comprehend the vicissitudes of network traffic, detect aberrant behavior, anticipate potential security threats, and can even optimize the allocation of network resources. For instance, within the realm of network traffic management, adaptive learning algorithms can project network load based on historical and real-time data, assisting network administrators in the real-time modulation of resources to guarantee a seamless and consistent digital experience for

users. During this robust self-regulating process, technologies like unsupervised learning often play pivotal roles, enabling predictive models to autonomously discover correlations within data without the need for manually tagged data. By employing various machine learning algorithms, including deep learning and reinforcement learning, these models explore and identify optimal solutions, equipping themselves to self-adjust in the face of novel data with proven recognition of the unknown. In epochs when networks encounter exponential data growth, adaptive learning and predictive models become particularly crucial. They exhibit unique advantages in the realm of network security; for instance, within intrusion detection systems, predictive models can detect threats in a timely manner by noting subtle changes in network behavior, swiftly recognizing and categorizing even unprecedented methods of attack. Silently, they stand as vigilant sentinels of network security. Moreover, in network operations, these models, through continuous learning of network status, can predict and forestall potential failures and proactively engage in troubleshooting and fault recovery, thus significantly enhancing network stability and reliability.

5. Conclusion

The synergistic interplay between big data and artificial intelligence heralds boundless prospects for the advancement of computer networking technology. By delving deeply into its applications within the realms of network security, administration, data analytics, and even cloud computing, artificial intelligence is rapidly becoming an indispensable catalyst for the intellectualization of computer networks. Nevertheless, an array of challenges remains to be confronted, including safeguarding the privacy and security of data, augmenting the transparency and interpretability of AI systems, and determining the optimal collaboration with human expertise. Looking ahead, technological innovations will persist in propelling the maturation of computer networks within these domains, all whilst placing a heightened emphasis on the integration of artificial intelligence with vast data repositories, thereby catalyzing societal progression as a whole.

References

[1] Yajuan Z ,Ru J ,Xiang J , et al. Application of wireless sensor network technology based on artificial intelligence in security monitoring system[J].Open Computer Science, 2023,13(1):205-212.

[2] Zhang Y. Research on the Application of Artificial Intelligence Technology in the Field of Network Security [J]. Journal of Artificial Intelligence Practice, 2023,6(6):88-100.

[3] Cheng L. Design and implementation of computer network security protection system based on artificial intelligence technology[J].Applied Mathematics and Nonlinear Sciences, 2023, 8(2):1491-1508.

[4] Jun P, JunYeong K, JunHo H , et al. A Novel on Conditional Min Pooling and Restructured Convolutional Neural Network[J].Electronics,2021,10(19):2407-2407.

[5] Lei Z ,Zening C ,Shufeng Y .Application of artificial intelligence in computer network security[J].Journal of Physics: Conference Series,2021,1865(4):1099-1108.

[6] Qing K. Face Image Feature Extraction based on Deep Learning Algorithm[J].Journal of Physics: Conference Series, 2021, 1852(3):608-615.