ISSN: 2754-6705

Journal of Mathematical & Computer Applications

SCIENTIFIC Research and Community

Review Article

Open Access

A Comprehensive Review of Named Data Networking: Architectural Principles, Techniques, Applications, Challenges and AI Integration

Sura Haidar Ali* and Alaa Shawqi Jaber

Information Networks Department University of Babylon, Iraq

ABSTRACT

Named Data Networking (NDN) paradigm is a novel approach to architecturally designing the internet. Instead of the traditional focus on the endpoints of the data, it will allow end-to-end communication based on the data itself. As a result, the NDN paradigm will provide significantly greater flexibility, scalability, and security compared to today's IP-based paradigm. This paper examines the fundamental elements of NDN, including the primary aspects of naming, routing, and caching that are essential to effective dissemination of data and distribution of content within distributed networks across multiple application domains. In addition to the examination of these elements, this paper reviews potential implementations of NDN within application domains such as IoT, multimedia streaming, vehicle networks, and smart city networks. While there are many challenges associated with implementing NDN applications, such as complexities of naming, scaling routing tables, and developing policies for privacy and cache management, this paper also reviews the use of artificial intelligence (AI) to improve NDN. Specifically, this paper reviews how AI can be applied to solve problems such as intelligent caching, adaptive forwarding, intrusion detection, etc. Additionally, this paper reviews how AI can improve network optimization using AI-driven NDN and demonstrates how AI-driven NDN can be used to create the next generation of intelligent and secure Internet architectures.

***Corresponding author**

Sura Haidar Ali, Information Networks Department University of Babylon, Iraq.

Received: August 07, 2026; **Accepted:** August 19, 2026; **Published:** August 24, 2026

Keywords: Named Data Networking (NDN), Information-Centric Networking (ICN), Caching Strategies, Routing and Forwarding, Internet of Things (IoT), Artificial Intelligence (AI)

Introduction

The growing need for robust, reliable, and efficient networks capable of providing continuous service in the event of a failure is driving the development of new paradigms and mod-els for distributed networks beyond the present host-centric models currently in place. This has evolved a number of new paradigms for networking, including Named Data Networking, in which communications are based on the identifiers of content rather than host addresses, and artificial intelligence to improve the performance of the network [1,2]. The Named Data Networking paradigm represents a fundamental architectural shift away from naming hosts to directly naming the data; unlike IP-based networks that route data to specific host addresses, NDN routes data by name and therefore focuses on what the user requires, rather than where it is located [3]. This content-centric approach, unlike the traditional host-to-host communication model, naturally mitigates many of the issues prevalent in current IP infrastructures [4]. In NDN, users request named content via an interest packet, and the network responds with a digitally signed data packet from any cacheable node in the network that contains a cached version of that data, allowing highly flexible and efficient delivery and retrieval of content [5]. NDN enables caching within the network itself; this leads to lower waiting times, better bandwidth usage, lower latency, and improved performance during periods of high mobility and multicast communications. The properties provided by NDN would be highly advantageous in environments with low or no reliability of network connections, including Internet of Things (IoT) and vehicular networks [2,3]. What is interesting is that NDN provides security to content through its digital signatures. It is important to note that NDN secures the data itself and does not protect the entire channel by signing each data packet cryptographically. The digital signature of the data name increases the integrity of transmitted data in NDN [6,7]. Researchers have begun to apply AI to the core components of NDN to further enhance the adaptability and efficiency of NDN. Machine learning and deep learning techniques are being utilized to provide opportunities in predictive caching schemes, adaptive forwarding algorithms, anomaly detection, and semantic interpretation of content names. With AI-enabled NDN systems, the network can determine the popularity of the content it stores, forecast requests from users, and make real-time decisions regarding the forwarding of interest packets that adjust to changing conditions in the network [8]. Although NDN offers benefits such as name-based routing and in-network caching, it is susceptible to attacks such as Interest Flooding Attacks (IFA). AI can be applied to detect and respond to malicious activities much more effectively than using conventional methods that are rule-based [9]. The integration of AI and NDN is crucial to achieving a truly responsive, scalable, and secure next-generation internet.

The rest of this survey is structured in seven sections. Section 2 discusses the previous work of researchers. Section 3 elaborates on concepts of NDN architecture and AI in net-working. Section 4 presents AI roles and techniques relevant to networking.

Section 5 presented NDN applications. Section 6 discusses existing challenges, limitations, and unresolved issues in current approaches. The final section reveals a conclusion and outlines future research directions.

Related Work

This literature is a complete assessment of Named Data Networking (NDN), a leading Information-Centric Networking (ICN) architecture. In order to place this survey in a framework of prior work, the Related Work portion of the paper has been divided into two sections. The first section systematically evaluates the core foundational research associated with NDN, application-specific implementations of NDN, the most current AI-driven advancements across multiple aspects of NDN, as well as the significant security concerns of NDN. The second section evaluates existing surveys and comparative studies of NDN. Research articles were collected from well-known academic databases, including IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar. Papers published in recent years were prioritized to capture the most up-to-date developments in this rapidly evolving field. while work not directly related to NDN or AI integration was excluded.

Foundational Studies and Recent Advances in NDN

In authors explore the architectural properties and attributes of Named Data Networking (NDN), such as the caching of content and intelligent packet forwarding in terms of a Content Delivery Network (CDN) workflow [5]. In IoT-based smart environments, NDN has considerable advantages. Raza et al. [3] introduced the INF-NDN IoT framework. They utilize NLP techniques such as LDA in order to optimize content names, retrieve semantics, and forward using semantics assisted by semantic tags, reducing name sizes by 40.05% and retrieval times. Campolo established Named AI Networking, which takes advantage of NDN traffic caching and semantic naming in order to support the orchestration of edge AI and inference results effectively, considerably reducing computation and latency [10]. Hail investigated the potential for employing AI technologies in IoT based NDN applications to manage large-scale data through adaptive intelligent decision-making through machine learning methods and reinforcement learning towards enhancement of caching, forwarding, routing, and energy management [8]. Xing proposed RL-ICN-CC, a deep reinforcement learning (DRL) congestion control algorithm for SDN-NDN satellite networks employing global state information for adaptive rate control in addition to redesigned FIB/PIT structures to address the effects of intermittent connectivity [11]. New vulnerabilities are introduced with NDN, such as interest flooding and cache pollution attacks. A method of detecting malicious Interest packets was proposed by Xing named RFDM, which is based on Reconstruction Forest, to analyze reconstruction error in PIT state and therefore detect malicious Interest packets [12]. A machine learning approach to detect interest flooding attacks in VNDNs was presented by Magsi in which they employed a random forest classifier to achieve an accuracy of 94% in distinguishing between legitimate and malicious vehicles [9]. Hidouri also developed a method called Q-ICAN, which employs Q-learning to predict cache pollution attacks, employing metrics such as cache hit ratio variation and interest inter-arrival times to achieve an accuracy of 95.09%. Table I summarizes the existing foundational studies and recent advances in the target area [13].

Table 1: Comparison of the Contribution of Foundational Studies and Recent Advances in NDN

Year	Ref.	Focus/Contribution	Key Aspec
2020	[5]	Explored caching and in-telligent packet forward-ing in NDN as part of a CDN workflow	Architectural features
2024	Raza et al. [3]	Proposed INF-NDN IoT using NLP (LDA) for se-mantic name optimization and tag-assisted forward-ing.	IoT and se-mantic nam-ing
2020	Campolo et al. [10]	Introduced "Named AI Networking" utilizing NDN caching and semantic naming for edge AI orchestration.	AI and edge computing
2024	Hail et al. [8]	Explored AI in IoT-based NDN for adaptive decision-making using ML and RL for caching, routing, and energy management.	AI and IoT optimization
2023	Xing et al. [11]	Proposed RL-ICN-CC, a DRL-based congestion control for SDN-NDN satellite networks.	DRL and congestion control
2024	Xing et al. [12]	Developed RFDM using Reconstruction Forest to detect malicious Interests via PIT analysis.	Security / In-terest Flood-ing Attack
2023	Magsi et al. [9]	Employed ML (Random Forest) for detecting In-terest Flooding in VNDN with 94% accuracy.]	Security / ML-based detection
2023	Hidouri et al. [13]	Proposed Q-ICAN using Q-learning for Cache Pol-lution Attack prediction with 95.09% accuracy.	Security / CPA mitigation

Related Surveys

Islam have outlined the appropriateness of NDN for smart environments since it reacts to information requests through an interest-based packet structure, whereby routers retrieve, forward, and track the requested packets and data via cache for speeded responses [6]. Rehman produced a detailed study of NDN architecture, naming, caching, routing, forwarding, and security [7]. The authors described a comparative taxonomy of approaches to these problems and identified key research areas that require additional work.

Also, performed a survey of the use of blockchain technology with NDN and demonstrated how the use of blockchain can potentially be used to provide enhanced decentralized architecture, scalability, and hierarchical access control [14]. In it was indicated that NDN is one of the most promising architectures to be developed as a future Internet architecture due to scalability, forwarding speed, trust models, network security, content protection, and privacy concerns [15]. The authors studied forwarding strategies, network models, simulation tools, and adaptive forwarding schemes and provided insight into the development of future NDN testbeds. Karim performed a comprehensive survey of routing strategies for NDN and compared different paradigms [16]. The authors also identified key open issues related to routing scalability. As a result of the functional complexity of NDN, there has been a specific focus on both the partitioning and optimization of NDN's core functions specifically, routing, forwarding, and caching. Nour did a survey that covered all aspects of access control (AC) mechanisms in NDN, which classified solutions based on whether or not they utilized encryption as part of their solution [17]. Although numerous surveys have explored various aspects of Named Data Networking (NDN), including its architecture, applications, and security mechanisms, there remains a noticeable gap in comprehensive studies addressing the integration of Artificial Intelligence (AI) within NDN. Table II summarizes the existing surveys in the target area.

Table 2: Comparison of the Contribution of Related Survey Papers

year	Ref.	Focus/Contribution	Key Aspec
2025	Islam et al. [6]	Discussed NDN suitabil-ity for smart environ-ments.	Smart environments
2020	Rehman et al. [14]	Surveyed NDN architecture, naming, caching, routing, forwarding, and security.	General NDN survey
2020	Rehman et al. [7]	Reviewed NDN- blockchain integration for decentralization, scalability, and access control.	Blockchain integration
2021	[15]	Analyzed NDN scalability, trust, security, privacy, forwarding strategies, and simulation tools.	Network modeling and performance
2022	Karim et al. [16]	Surveyed NDN routing strategies; compared paradigms and identified open challenges in scalability.	Routing-focused survey
2020	Nour et al. [17]	Covered access control (AC) mechanisms in NDN, classifying solutions with and without encryption.	Access control and pri-vacy

NDN Architecture and AI Integration

Over time, the shortcomings of conventional IP-based net-work architectures have become clearer as the need to have fast, scalable, and secure communication of data increases. NDN takes networks in a new direction by relying on a data-driven rather than host-based networking paradigm, resulting in new mechanisms, including name-based routing, in-network caching, and data-centric security. The following sections offer an overview of the NDN architecture with a focus on the potential and role of Artificial Intelligence (AI) in improving its core functionalities.

NDN Architecture

Named Data Networking (NDN) is a data-centric, receiver-driven network architecture that operates based on content names rather than host addresses. It emerged from the ear-lier Content-Centric Networking (CCN) project introduced in 2009 by Jacobson and later evolved under the NSF-funded Future Internet Architectures (FIA) program between 2010 and 2016 [6]. At the core of the NDN model is a pull-based communication paradigm. Done by three main tables in NDN that are used to perform its functions. Content Store (CS): caches a copy of data packets in order to save bandwidth as well as improve the ability to share content with others and retrieve data more quickly than retrieving it directly from the source. Pending Interest Table (PIT): tracks all interest packets and which interface they came into until the data is received back and/or the interest packet expires. Forwarding Information Base (FIB): stores the next hop for all interest packets so that they can be forwarded appropriately [18]. The consumer applications generate interest packets based on the name of the data chunk they are interested in. Then comes the network role to forward the interest packets using the Forwarding Information Base (FIB), with intermediate routers maintaining a Pending Interest Table (PIT) to keep track of outstanding requests. When a data packet is found, it is sent through the reverse path of the PIT and returned to the source. This process is governed by the flow balance principles of the NDN solution, which means that each interest can only get one data packet and that the PIT entries that go with it are used up after that Fig. 1 [6,7,19].

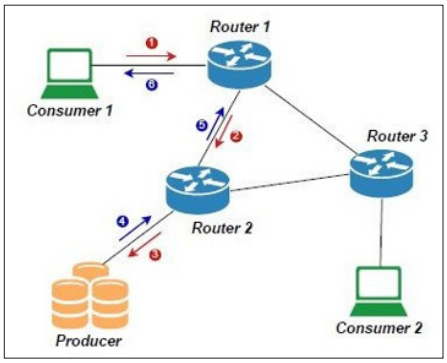

Figure 1: NDN forwarding model [20]

The NDN forwarder has a component called a Content Store (CS), which caches the data packets that it receives. When the same content is requested again via Interests, the requests can be satisfied from the cache, thus improving retrieval latency and reducing redundant transmissions. With cached data identified both by name and a cryptographically generated signature, each packet can be independently validated, with no reliance on source information NDN names have a hierarchical structure similar to HTTP URLs, consisting of several name components; for example, a content name might be in the form "/domain/audio/audio A/mp3," which reflects the identity and context of the content [2,21,22]. Overall, the main features of NDN, such as semantic naming, stateful for smart environ Mensching, and data-centric security, position it as a strong candidate for the next generation of Internet architectures, particularly in devices that will require a good system of distribution to be made part of demanding applications such as the IoT and Smart Environments [8].

Artificial Intelligence Integration with NDN

Artificial Intelligence (AI) is transforming the world of networks quickly through dynamically adaptive, intelligent, and automated mechanisms, which are impossible to achieve with traditional approaches [23-25]. The infusion of Artificial Intelligence (AI), such as Machine Learning (ML) and Deep Learning (DL), has radically altered the nature of Named Data Networking (NDN) and is positioning this paradigm as a key enabler in the adaptability and efficiency of future network architecture, especially in dynamic, changing environments like the Internet of Things (IoT) [26]. AI-driven techniques are essential to solving the complexities of modern networking by improving data processing methods as well as providing for smart networks, which possess the ability of dynamic decision-making and real-time processing [27-29]. This intelligence is being applied in a systematic way to enhance many prime functionalities of NDN, such as caching strategies, forwarding and routing decisions, and optimizing energy consumption [8,30] as illustrated in Fig. 2 AI is also employed to promote and innovate security measures for protecting the network against unique threats stemming from the NDN, such as the Interest Flooding Attack (IFA) [9-31]. Furthermore, NDN is observed to have suitable features that permit the implementation of Edge AI technology by allowing in-network placement, discovery, and chaining of various AI components, which include models, parameters, and inference results, permitting local, low-latency data processing [10]. However, additional computational overhead may introduce by integrating AI models into NDN environments, particularly when deployed on resource-constrained routers and IoT devices. Many AI and deep learning models demand significant processing power, memory, and energy for training and inference. As a result, implementing such models directly within NDN nodes may lead to higher processing latency and energy usage [8].

Common AI Techniques Used in NDN

Artificial Intelligence (AI) has become a transformative technology within Named Data Networking (NDN), which enables efficiency through intelligent automation and adaptive decision-making in core areas of important functionalities such as caching, forwarding, routing, congestion control, and security. Furthermore, these techniques make NDN more scalable, adaptive, and efficient for current networking requirements. Table III summarizes common AI techniques used in NDN.

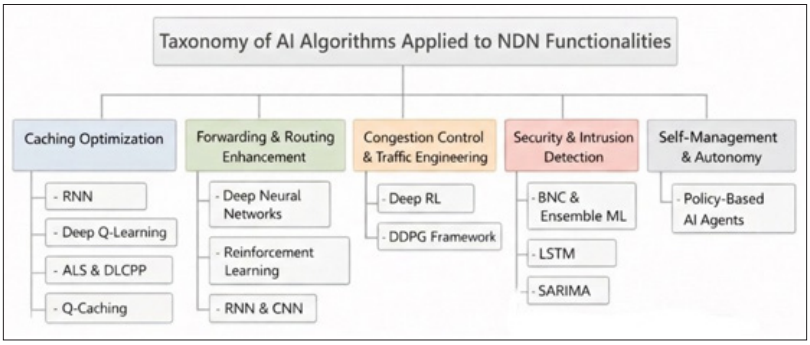

Figure 2: Taxonomy of AI Algorithms Applied to NDN Functionalities

Table 3: Common AI Techniques Used In NDN

Category	Techniques/Tools	Description (Use in NDN)	Ref.
Caching Optimization	RNNs, DQL, ALS, DLCPP, ANN, Q-caching	Predict content popularity, optimize caching, reduce latency and support caching/routing decisions.	[8], [30]
Forwarding & Routing Enhancement	DNNs, RNNs, CNNs, RL	Enable adaptive routing and optimize forwarding under dynamic conditions.	[23], [32]
Congestion Control & Traffic Management	DRL, DDPG (DRL-TE Framework)	Manage congestion, improve link utilization, and reduce delays.	[11]
Security & Intrusion Detection	BNC, LSTM, SARIMA	Detection of cache poisoning and interest flooding attacks.	[33]
Self-Management & Autonomy	Policy-based AI agents, Autonomous Systems	Enable self healing, resource optimization, and autonomous operation.	[32]

Caching Optimization

AI models, especially machine learning or deep learning techniques, play a prominent role in predicting content popularity and dynamically managing cache storage. For example, models driven by AI predetermine which data objects are most likely to be requested by IoT-NDN devices and use previous access patterns to prefetch the likely objects [8]. This is also the situation in ordinary NDN environments. Machine learning techniques such as Recurrent Neural Networks (RNNs) and Deep Q-Learning (DQL) are effectively applied to improve content caching strategies. The result of these techniques is increased cache hit ratios, and by predicting content popularity and making optimal caching decisions, indirectly, a reduction in the latencies associated with content retrieval. Several studies have proposed intelligent caching strategies that involve using AI techniques such as Alternating Least Squares (ALS) for the future prediction of ratings and Deep Learning approaches for Content Placement Policies (DLCPP) in SDN-NDN. The author particularly emphasizes the use of an overlap network based on Artificial Neural Networks (ANN) to provide a lightweight caching scheme. Furthermore, Q-caching, an approach based on reinforcement learning, supports cache and routing through reductions in both the end user download time and custodial load [30].

Forwarding and Routing Enhancement

In NDN, forwarding and routing gain advantage from deep learning and reinforcement learning models, which are adept at real-time decision-making. In the context of network routing, decisions will be assisted regarding content-based routing by examining the properties of the contents using deep neural networks. In addition, reinforcement learning agents can optimize forwarding techniques based on network conditions and content needs. One study has also shown that deep learning can process traffic patterns based on historical data to yield decisions for adaptive routing using RNNs and CNNs methods [23,32].

Congestion Control and Traffic Management

Plenty of researchers have applied artificial intelligence to congestion control. NDN networks make use of deep reinforcement learning techniques to manage network congestion and come up with optimization solutions in real time, especially when combined with SDN [11]. According to create a framework, DRL-TE, based on a reinforcement learning deep deterministic policy gradient (DDPG) [34]. In the experiment, according to the link bandwidth, it was shown that the utilization of the link is improved and the end-to-end delay is down, but there was no comparison in the experiment with the dynamic network. These techniques allow the network to dynamically control the data flows without rigid threshold systems to regulate the flows at the moment, resulting in more uniform traffic distributions and less bottlenecking in times of high demand.

Security and Intrusion Detection

AI also plays a role in the security of the NDN network, particularly for the detection of Cache Poisoning Attacks (CPA) and Interest Flooding Attacks (IFA). As shown in it was stated that the ML solution developed by Montimage exploits ensembles of ML models organized in a Bayesian Network Classifier (BNC) for monitoring the behavior of nodes in the NDN topology. Each of the nodes is equipped with probes that will collect metrics such as the Content Store (CS) and Pending Interest Table (PIT), which will be cross-correlated to detect abnormal behavior. Furthermore, it would be the hybridization approaches, such as the Long-Short Term Memory (LSTM) and Seasonal Autoregressive Integrated Moving Average (SARIMA), which are statistical and deep learning, offering a system of future-proofing combining the benefits of time-series forecasting and adaptive modeling in order to reduce false alarms and more quickly and appropriately detect intrusions, which is so important in today's cybersecurity based on NDN [33].

Self-Management and Network Autonomy

AI makes it possible for NDN to manage its own network through policy-based automation and self-healing procedures. As noted in an autonomous system can actually help in better utilization of the resource, fewer overheads to be tackled, and the overall reliability of the network." AI agents are capable of detecting failures, analyzing root causes, and restoring services without human intervention. Such autonomy is essential for future NDN-based infrastructures that must scale to millions of nodes and support dynamic user mobility, high throughput, and low latency [32].

Applications of Named Data Networking (NDN)

Named Data Networking (NDN) goes beyond a networking paradigm and aims to enable innovative applications in a variety of different areas. NDN provides inherent benefits such as in-network caching, data-centric security, and support for mobility by virtue of naming data instead of hosts. As indicated in Fig. 3, these benefits give NDN increased utility in many current and future applications, including content and multimedia distribution; Internet of Things (IoT) and intelligent environments; vehicular networks; real-time healthcare systems, and solutions centered upon security.

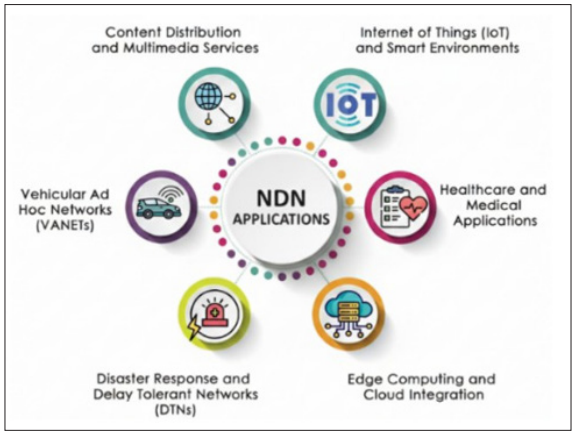

Figure 3: NDN Applications

Content Distribution and Multimedia Services

Named Data Networking (NDN) represents a powerful technology for multimedia and content dissemination, primarily through its receiver-driven communication model, in-network caching, and semantic naming. In the case of live streaming, PC Live is designed to use NDN as a distribution mechanism, converting HTTP Live Streaming (HLS) into NDN. PC Live has been developed using open-source tools such as Shaka Player and OBS and has been tested on a large-scale, multi-city NDN testbed. The results from this testbed demonstrate that PC Live is capable of serving up to 3.95 times more clients than an equivalent IP-based livestreaming service in a comparable environment and is able to consume 34.8 percent less bandwidth than the IP-based service on the bottleneck link [35]. Decentralized photo sharing represents another example of the benefits provided by NDN. While current cloud-based photo-sharing apps are highly dependent upon cloud services, a design based on NDN provides a means of implementing a decentralized solution that does not rely on central servers [36].

Finally, NDN can also be seen to align well with the general goals of Content Delivery Networks (CDNs), including seamless failover, partial data retrieval, through the location independence it affords [5].

Internet of Things (IoT) and Smart Environments

IoT enables objects that are part of everyday life to be connected to the internet so they may exchange information via small, low-power units that contain sensors and actuators. There are challenges to implementing IoT, including limited power supply, bandwidth limits, and security risks [8]. With the development of IoT for smart environment ecosystems, there has been an understanding of the limitations of traditional IP-based networks. NDN, as a result of its data-centric approach to networking, provides solutions to the limitations of traditional IP networks with regard to scalability, mobility, and efficiency using hierarchical naming, in-network caching, built-in security, and mobility mechanisms such as prefix delegation and anchor-based routing. Additionally, NDN enables a fine-grained access control system to enable data sharing to be secure within smart environments [6]. Moreover, by optimizing parameters of IoT-NDN, such as network size and packet format, significant reductions in energy consumption may occur, with the assistance of simulation tools such as NDNSIM [37]. The integration of artificial intelligence (AI) into IoT-NDN architectures can increase the predictability of traffic patterns, further increase the efficiency of data transfer, and increase the security of IoT systems via anomaly detection and encryption [8]. Together, NDN and AI represent a scalable, secure, and efficient foundation upon which smart infrastructure of the next generation may be developed.

Vehicular Ad Hoc Networks (VANETs)

Due to VANETs' highly dynamic network topologies, very frequent disconnection events, and unreliable broadcasting channels, it is difficult to perform multi-hop content retrieval efficiently. However, since the architecture of NDN is designed to support both native multicast, mobility, and data-centric security, NDN's architecture fits well with the characteristics of VANETs, where vehicles operate under a high degree of mobility and in a dynamic environment [38,39]. NDN has advantages but has some security issues when used on VANETs. NDN is resistant to many types of IP-based DDoS attacks but creates other types of vulnerabilities, such as flooding of unnecessary interest messages, distribution of false data that could exhaust system resources, or cache pollution. Also, semantic correlation in how human-readable names are created for NDN entries may make them trackable or subject to censorship [40].

Healthcare and Medical Applications

Named Data Network (NDN) is a rapidly developing paradigm for healthcare advancement via intelligent and efficient content retrieval, in-network caching, security by de-sign, and built-in support for mobility and scalability. The secured communication pattern, being a content-centric approach, helps to advance many healthcare applications like pandemic management and remote patient monitoring. Less latency and improved accessibility to data and information within the resource-constrained environments by the communication infrastructure, like healthcare, may be in the Internet of Things (IoT) or, for example, the Internet of Healthcare Things (IOHT). Incorporating the NDN paradigm into IoT enhances the opportunity to rapidly communicate information and address the health emergencies of disease outbreak management during pandemics [41,42]. On the other hand, to improve the security of IoT-enabled healthcare (IOTEH) by offering a framework called Identity-Based Signcryption (IBS) that uses HCC (Hyperelliptic Curve Cryptosystem), reducing dependence upon legacy public key infrastructure, and providing NDN-IoT device performance improvements [43]. Mobile health (mHealth) applications also make use of the features of the Named Data Networking (NDN) architecture to address challenges in real-time data sharing and fine-grained access control over contextual information [44]. Finally, NDN shows its potential to increase the efficiency, security, and responsiveness of modern healthcare systems.

Disaster Response and Delay Tolerant Networks (DTNs)

Damaged infrastructure, intermittent connectivity, and high responder mobility often hinder communication, while IP-based systems struggle with role-based communication and dynamic mobility. Named Data Networking (NDN) addresses these challenges by routing data based on content names rather than IP addresses, enabling location-independent, role-based group communication among responders. With its in-network caching, multipath routing, and adaptive forwarding, NDN enhances resilience and mobility in disrupted networks [45]. On the other hand, due to the nature of DTNs, NDN is well-suited for supporting both secure and efficient data delivery in intermittent connectivity scenarios by providing an inherent ability for consumers to receive their requested data from any available cache location in the network [46]. Military multi-UAV surveillance systems, as well as Catastrophic Terrestrial Environments and Extraterrestrial Environments, are all DTN applications that apply to NDN. An NDN-based solution allows for the flexible deployment of customized network functionality during operation, enabling rapid node replacement as well as localized retrieval of content via caching critical for many types of tactical missions requiring low-latency video and/or image delivery. Similarly, in space-based DTM communications such as LEO satellite constellations [47,48].

Edge Computing and Cloud Integration

Edge computing and cloud computing enable NDN-based IoT systems to be more efficient, as they bring computation and storage much closer to the device. Through the use of NIOTE, IoT devices will cache and process locally collected data at their local edge node, enabling NDN in network caching and request aggregation to provide access to data via a single communication process from the nearest provider, resulting in lower latencies and costs [49]. Moreover, NDN's caching is inherently compatible with edge computing because it allows nodes to deliver data directly from the node's cache store without needing to interact with the cloud frequently. This method of delivering data will result in increased performance, lower latency, and reduced energy consumption, which are common reasons why edge computing is preferred to cloud computing in IoT deployments using NDN [42,50].

Key Issues and Open Challenges

While Named Data Networking (NDN) offers a number of advancements to performance, scalability, and security, as well as through the combination of named data networking and artificial intelligence (AI), it has been met with several technical, operational, and architectural impediments that are preventing it from being adopted at scale. The impediments include interoperability, mobility management, security, caching optimization, and AI integration, as described in Table IV entitled Key Issues and Open Challenges with NDN [51-53].

Table 4: Key issues and Open Challenges with NDN

Category	Description	Key Ref.
Interoperability & Standardiza-tion	Legacy device compatibility (data-centric vs. channel-based security), absence of universal naming/packet/security standards, need for efficient NDN–IP gateways, limited testbeds.	[6]
AI Integration in NDN	Increased computational over-head on resource-constrained nodes.	[8]
Mobility Management	Producer handoff latency, signaling costs, outdated FIB, need for joint consumer–producer mobility with secure, fast handoffs.	[51]
Security Threats	vulnerable to many attacks.	[52], [53]
Caching Optimization	Popularity manipulation, redundancy and diversity trade-offs, CS lookup scalability, en-ergy -aware cache placement in mobile/wireless.	[53]

Conclusion

Named Data Networking is a disruptive paradigm in how we can achieve an optimized, intelligent, and secure Inter-net Architecture. Integrating Artificial Intelligence (AI) with Named Data Networking will provide significant opportunities for NDN to adaptively cache content, make intelligent routing decisions, and automatically detect threats. To realize this potential, however, researchers need to pursue several key challenges in NDN, including developing a scalable and dynamic naming system; designing a mechanism to perform private and/or anonymous data retrieval; creating energy efficient caching solutions that are applicable to IoT and mobile devices; and developing AI-based optimization algorithms that enable real-time decision making. In addition, pursuing the integration of NDN across layers with emerging technologies such as edge computing, blockchain, and 6G networks will allow us to move toward the development of future context-aware Internet architectures. These paths will allow Named Data Networking to evolve into a self-sufficient and autonomous framework to support the needs of future intelligent communication systems.

References

1. A Afanasyev, J Burke, T Refaei, L Wang, B Zhang, et al. (2018) A brief introduction to named data networking. IEEE Military Communications Conference https://named-data.net/publications/ndn18/
2. W Azamuddin, A Aman, H Sallehuddin, K Abualsaud, N Mansor (2023) The emerging of named data networking Architecture application and technology. IEEE Access 11: 23620-23633.
3. G Raza, I Ullah, M Din, M Rehman, B Kim (2024) Inf-NDN IoT An intelligent naming and forwarding in name data networking for internet of things. IEEE Access 12: 114319-114337.
4. H Liu, R Han (2021) A hierarchical cache size allocation scheme based on content dissemination in information-centric networks. https://ideas.repec.org/a/gam/jftint/v13y2021i5p131-d555354.html.
5. R Thelagathoti, S Mastorakis, A Shah, H Bedi, S Shannigrahi (2020) Named data networking for content delivery network workflows. IEEE 9th International Conference on Cloud Networking Cloud Net https://susm.it/publication/content/publication/thelagathoti-2020-named/.
6. R Islam, C Savaglio, G Fortino (2025) Leading smart environments towards the future internet through name data networking A survey. Future Generation Computer Systems https://www.sciencedirect.com/science/article/pii/S0167739X25000494.
7. K Asaf, R Rehman, B Kim (2020) Blockchain technology in named data networks A detailed survey. Journal of Network and Computer Applications 171: 102835-102840.
8. M Hail, A Bin Salem, W Munassar (2024) AI for IoT-NDN Enhancing IoT with named data networking and artificial intelligence. ICETSIS 1020-1026.
9. A Magsi, S Mohsan, G Muhammad, S Abbasi (2023) A machine learning-based interest flooding attack detection system in vehicular named data networking. Electronics 12: 3860-3870.
10. C Campolo, G Lia, M Amadeo, G Ruggeri, A Iera, et al. (2020) Towards named AI networking Unveiling the potential of NDN for edge AI. International Conference on Ad-Hoc Networks and Wireless Springer.
11. Z Xing, H Qi, X Di, J Liu, L Cong (2022) Deep reinforcement learning based congestion control mechanism for SDN and NDN in satellite networks International Conference on Mobile Wireless Middleware Operating Systems and Applications Springer.
12. G Xing, X Li, R Hou (2024) A reconstruction forest-based interest flooding attack detection method in named data networking. International Conference on Computing Networking and Communications http://www.conf-icnc.org/2024/papers/p823-xing.pdf.
13. A Hidouri, H Touati, M Hadded, N Hajlaoui, P Muhlethaler, et al. (2023) Q-ICAN A Q-learning based cache pollution attack mitigation approach for named data networking. Computer Networks 235: 109990-109998.
14. V Singh, R Ujjwal (2020) A walkthrough of name data networking Architecture functionalities operations and open issues. Sustainable Computing Informatics and Systems 28: 100410-100419.
15. S Ahdan, A Nurhayati, G Nurkahfi, N Syambas (2021) Adaptive forwarding strategy in named data networking A survey. 15th International Conference on Telecommunication Systems Services and Applications https://www.academia.edu/75068918/Adaptive_Forwarding_Strategy_in_Named_Data_Networking_A_Survey.
16. F Karim, A Aman, R Hassan, K Nisar, M Uddin (2022) Named data networking A survey on routing strategies. IEEE Access 10: 90254-90270.
17. B Nour, H Khelifi, R Hussain, S Mastorakis, H Moungla (2021) Access control mechanisms in named data networks A comprehensive survey. ACM Computing Surveys 54: 1-35.
18. K Ahmed, R Rehman, K Kim (2024) Caching strategies in NDN based wireless ad hoc network A survey. Computers Materials & Continua 80: 50-61.
19. A Mtibaa, S Mastorakis (2020) NDNTP A named data networking time protocol. IEEE Network 34: 235-241.
20. E Bardhi, M Conti, R Lazzeretti, E Losiouk, A Taffal

(2022) Sim2testbed transfer NDN performance evaluation. Proceedings of the 17th International Conference on Availability Reliability and Security 26.

21. M Shah, Y Leau, Z Yan, M Anbar (2022) Hierarchical naming scheme in named data networking for internet of things A review and future security challenges. IEEE Access 10: 19958-19970.
22. J Kim, M Ko, M Shin, J Kim (2020) Scalable name lookup for NDN using hierarchical hashing and Patricia trie. Applied Sciences 10: 1020-1023.
23. C Mavani, H Mistry, R Patel, A Goswami (2024) Artificial intelligence AI based data center networking. International Journal on Recent and Innovation Trends in Computing and Communication 12: 508-518.
24. U Prabhakara, D Yadav (2023) The role of AI in the development of next-generation networking systems. The Role of AI in the Development of Next-Generation Networking Systems 15: 1048-1059.
25. M Maaroof, N Al-Msarhed, A Jaber (2025) Fractal-hyper net Elevating X-ray diagnostic visualization through deep hyper-dimensional feature learning and fractal-scale structural integrity. Journal of Internet Services and Information Security 15: 871-891.
26. I Abbood, A Idrees (2023) A literature review on data transmission reduction techniques for wireless multimedia sensor networks. 14th International Conference on Computing Communication and Networking Technologies 36.
27. A Ali, A Abdullah (2025) Text email spam adversarial attack detection and prevention based on deep learning International. Journal of Intelligent Engineering & Systems 45.
28. M Mohammed, Z Abod, A Abdullah (2022) Secure SDN traffic based on machine learning classifier LC. International Journal of STEM 3: 118-128.
29. M Bashaa, W Bhaya, N Al-Aaraji (2025) Integration of zero trust architecture and machine learning for improving the security of software defined networking A review. Journal of Intelligent Informatics Networking and Cybersecurity 1: 1-20.
30. R Negara, N Syambas (2020) Caching and machine learning integration methods on named data network A survey. 14th International Conference on Telecommunication Systems Services and Applications 65.
31. A Agiollo, E Bardhi, M Conti, R Lazzeretti, E Losiouk, et al. (2023) GNN4IFA Interest flooding attack detection with graph neural networks. IEEE 8th European Symposium on Security and Privacy Euro S&P 25.
32. H Mistry, C Mavani, A Goswami, R Patel (2024) Artificial intelligence for networking. Educational Administration Theory and Practice 30: 813-821.
33. G Apruzzese, P Laskov, E Montes de Oca, W Mallouli, L Brdalo Rapa, et al. (2023) The role of machine learning in cybersecurity. Digital Threats Research and Practice 4: 1-38.
34. Z Xu, J Tang, J Meng, W Zhang, Y Wang, et al. (2018) Experience-driven networking A deep reinforcement learning based approach. IEEE Conference on Computer Communications 53.
35. T Liang, W Huang, X Ma, W Zhang, Y Zhang, et al. (2023) PC Live Bringing named data networking to internet livestreaming. Proceedings of the 10th ACM Conference on Information-Centric Networking 65.
36. V Patil, T Yu, X Ma, L Zhang (2023) Decentralized photo sharing via named data networking. Proceedings of the 10th ACM Conference on Information-Centric Networking 46.
37. D Papenfu, B Gerlach, S Fischer, M Hail (2024) Enhancing energy efficiency in IoT-NDN via parameter optimization. Future Internet 16: 55-61.
38. D Li, T Song, Y Yang (2020) Content retrieval based on prediction and network coding in vehicular named data networking. IEEE Access 8: 125576-125591.
39. G Araujo, M Peixoto, L Sampaio (2021) NDN4IVC: A framework for simulating and testing of applications in vehicular named data networking https://arxiv.org/abs/2107.00715.
40. S Signorello, M Palattella, L Grieco (2016) Security challenges in future NDN-enabled VANETs. IEEE 1771-1775.
41. M Khan, M Saad, M Tariq, J Akram, D Kim (2021) SPICE-IT Smart COVID-19 pandemic controlled eradication over NDN-IoT. Information Fusion 74: 50-64.
42. N Askar, A Habbal, H Hamouda, A Alnajim, S Khan (2024) SEF A smart and energy-aware forwarding strategy for NDN-based internet of healthcare. Computers Materials & Continua 26.
43. S Ullah, S Hussain, A Gumaei, H AlSalman (2021) A secure NDN framework for internet of things enabled healthcare. Computers Materials & Continua 49.
44. P Kar, K Chen, J Shi (2022) DMACN A dynamic multi-attribute caching mechanism for NDN-based remote health monitoring system. IEEE Transactions on Computers 72: 1301-1313.
45. M Tran, Y Kim (2021) Named data networking-based disaster response support system over edge computing infrastructure. Electronics 10: 330-335.
46. T Li, Z Kong, L Zhang (2020) Supporting delay tolerant networking A comparative study of epidemic routing and NDN. IEEE International Conference on Communications Workshops ICC Workshops 54.
47. O Da Cruz, C Pereira, A Da Silva, J Da Costa, P Mendes, et al. (2024) Dynamic deployment and control of an NDN network for military multi-UAVs based surveillance applications. International Conference on Unmanned Aircraft Systems 52-68.
48. T Liang, Z Xia, G Tang, Y Zhang, B Zhang (2021) NDN in large LEO satellite constellations A case consumer mobility support. Proceedings of the 8th ACM Conference on Information-Centric Networking 25.
49. X Wang, S Cai (2020) Secure healthcare monitoring framework integrating NDN-based IoT with edge cloud. Future Generation Computer Systems 112: 320-329.
50. X Wang, X Wang, Y Li (2021) NDN-based IoT with edge computing. Future Generation Computer Systems 115: 397-405.
51. Abrar A, Arif A, Zaini K, Omar M, Meng Y (2024) Advancing producer mobility management in named data networking A comprehensive analytical model. Journal of King Saud University Computer and Information Sciences 36: 102040-102045.
52. A Benmoussa, C Kerrache, N Lagraa, S Mastorakis, A Lakas, et al. (2022) Interest flooding attacks in named data networking Survey of existing solutions open issues requirements and future directions. ACM Computing Surveys 55: 1-37.
53. R Alubady, M Salman, A Mohamed (2023) A review of modern caching strategies in named data network Overview classification and research directions. Telecommunication Systems 84: 581-626.