IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 27 December 2022, accepted 29 January 2023, date of publication 6 February 2023, date of current version 13 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3243006

SURVEY

The Emerging of Named Data Networking: Architecture, Application, and Technology

WAN MUHAMMAD HAZWAN AZAMUDDIN[1], AZANA HAFIZAH MOHD AMAN[1], HASIMI SALLEHUDDIN[1], KHALID ABUALSAUD[2], (Senior Member, IEEE), AND NORHISHAM MANSOR[3]

[1]Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi 43600, Malaysia
[2]Department of Computer Science and Engineering, College of Engineering, Qatar University, Doha, Qatar
[3]Department of Electrical Technology, Advance Technology Training Center (ADTEC) Batu Pahat, Johor, Malaysia

Corresponding author: Wan Muhammad Hazwan Azamuddin (p101964@siswa.ukm.edu.my)

This work was supported by the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, FRGS/1/2019/ICT03/UKM/02/1.

ABSTRACT Named Data Networking (NDN) is developed to accommodate future-oriented internet traffic. In recent years, NDN's popularity has grown due to the evolution of the Internet of Things, Artificial Intelligence, Cloud Services, and Blockchain. NDN's key promising features are dynamic content management, privacy, mobility, and trust. This manuscript provides a comprehensive overview of the motivations and promises of NDN in the context of recent evolution technologies and applications. The recent reviews highlight the trend of NDN Blockchain and 5G technology with 73% of research interest, while transportation applications dominate 64% of the research interest. Afterward, we discuss existing NDN Architecture, Operation, Services, and applications, as well as the most popular NDN technologies. Our discussions are based on investigating current solutions with criticism. These significantly highlight the emergence of the NDN and the potential to revolutionize internet traffic management and security.

INDEX TERMS NDN AI, NDN application, NDN blockchain, NDN cloud edge, NDN IoT, NDN technology.

I. INTRODUCTION

Due to the expansion of the Internet, the Internet of Things (IoT), and new network technology in recent decades, the modern Internet has been forced to comply with even more demanding standards than its creators had envisioned. Accordingly, the efforts of academic and industrial professionals are focusing more on building the next-generation network, overcoming the new Internet's myriad flaws, and ensuring its long-term growth [1]. The massive data sharing and mobility support must tackle different aspects [2]. Statistics show that mobility traffic users will increase more than fixed IP traffic [3]. Shortly, there will be a large number of digital internet-enabled gadgets needing access in any location and at any time. Network architecture should provide dynamic mobility to ensure dependable connectivity and data availability anywhere. Because the traditional architecture, TCP/IP, is connection-oriented while going around in one connection, it causes additional network latency. The consumer must submit a request every time because there is an interruption.

Named Data Networking (NDN) caches content on all nodes, eliminating the need to constantly request content from the originating server. It demonstrates the advantages of a well-designed NDN infrastructure through various standard and new applications. NDN enables these qualities to implement reliable networks and applications due to the nature of the underlying architecture design. NDN can enhance performance by minimizing per-content cache consumption and providing a faster time to the first byte, which improves user experience [4]. Furthermore, NDN permits numerous mechanisms that are difficult to implement using IP addresses [5]. Additionally, partial data retrieval, the ability to automatically switch to a better path, transparent failover, and the

The associate editor coordinating the review of this manuscript and approving it for publication was Ting Yang.

TABLE 1. Article citation database.

Database & Indexing Body	Total	Ratio %
Web of Science	94	34.0
Scopus	104	37.0
IEEE Xplore	58	21.0
Science Direct	17	6.0
Technical Report & RFC	6	2.0

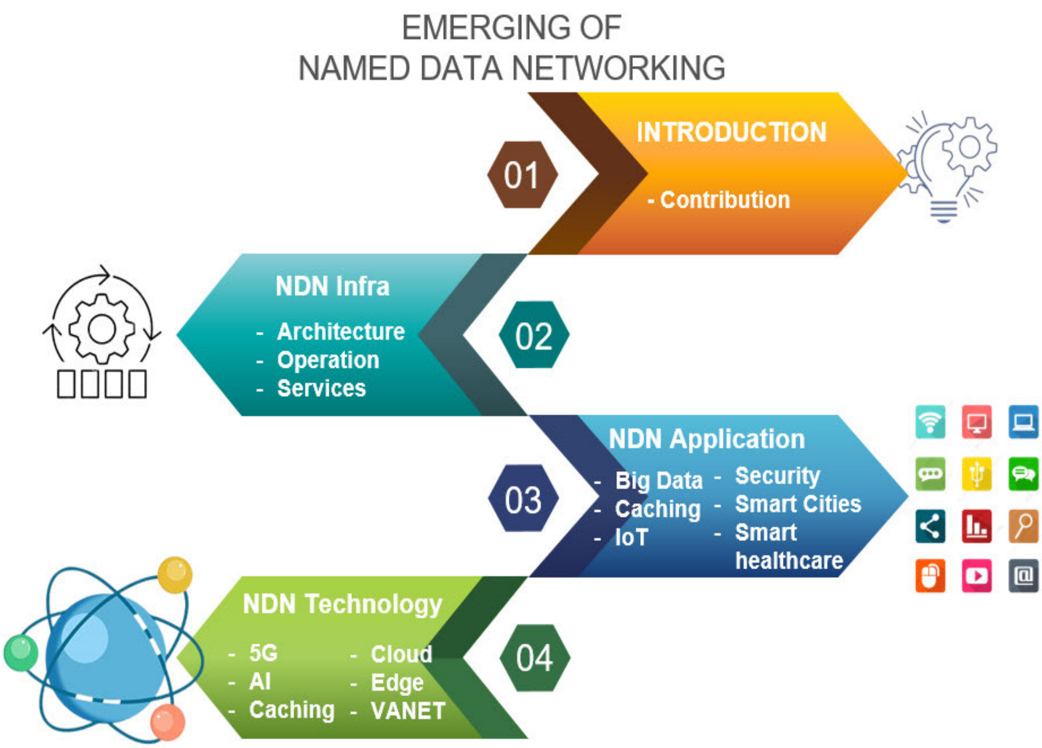

FIGURE 1. Organization of article.

ability to retrieve content from numerous sources are essential qualities that simplify an NDN infrastructure and improve user experience [6].

This article uses the following three widely known databases to find review and research articles: IEEE Xplore [7], Science Direct [8], RFC [9], and Google Scholar [10] for searching for an appropriate journal, proceeding, technical report, and RFC as shown in Table 1. Table 1 depicts the articles from Web of Science (34%), Scopus (37%), IEEE Explore (21 %), Science Direct (6%), and Technical Report & RFC (2%). A total of 133 research articles, 39 for the NDN Architecture, operation, and Services, 44 for the NDN application, and 50 for the NDN technology section. The following six keywords are "NDN AI", "NDN application", "NDN blockchain", "NDN Cloud Edge", "NDN IoT", and "NDN technology". All the extracted articles are selected based on the title, abstract and content relevancy.

Many NDN review papers have been conducted based on specific aspects of the NDN without any particular focus. Recent NDN review papers primarily examined NDN surface design and characteristics, leaving out information on NDN current technologies strategies and applications unresolved concerns. Thus, this paper aims to comprehensively describe the NDN emerging technologies and applications by considering research papers published from 2018 to 2022.

To be exact, the following are the contribution of this paper

1. An insight into the most relevant recent review publications on NDN applications from 2018 to 2022.
2. A concise and comprehensive overview of the standard and recent research of NDN architecture, operations, and services.
3. A highlight of the most recent and popular NDN technology research, including AI, Blockchain, Cloud, and IoT.

TABLE 2. Existing NDN review and survey areas.

Ref	Year	Area of concern	Application Scope				Technology Scope				
			Healthcare	Transportation	Entertainment	Security	IoT	AI	5G	Blockchain	Cloud
[11]	2018	Lightweight detection, protection, and mitigation technique	✖			✖	✖			✖	
[15]	2018	Transmission open issues and challenges		✖					✖		✖
[12]	2018	Security support on data authenticity, confidentiality, and availability	✖			✖				✖	
[13]	2019	Packet forwarding requirements and models			✖		✖		✖	✖	
[16]	2020	Caching strategy		✖	✖				✖	✖	✖
[17]	2020	Communication model		✖					✖		✖
[14]	2021	Bloom Filter			✖		✖				
[22]	2021	Data dissemination		✖			✖		✖	✖	
[19]	2021	Vicinity-based content finding	✖	✖			✖		✖	✖	
[20]	2022	Hybrid Information	✖	✖	✖		✖	✖	✖	✖	
[21]	2022	Hybrid cache Management	✖	✖	✖		✖	✖	✖	✖	
		Ratio	45%	**64%**	45%	64%	64%	18%	**73%**	**73%**	27%

Table 2 highlights in detail the coverage of the recent review papers. Based on the table, in 2018, the contribution is more towards mitigation techniques that cover healthcare applications with blockchain and security technology [11], [12]. Bloom filter techniques discussed for forwarding requirements focused on entertainment applications with IoT technology [13], [14]. Comprehensive reviews on vehicular NDN in 2018, 2020, and 2021 focus on transportation applications and cloud technology [15], [16], [17], [18], [19]. Latest findings and interest of research review on NDN hybrid techniques with 5G technology with healthcare and entertainment applications [20], [21].

The article has four major sections, as shown in Fig 1. Section I explains the NDN's introduction, including contribution, article selection method, and outline. Section II describes the NDN architecture and operation and summarizes NDN services. Section III demonstrates the NDN application that covers the Internet of Things, smart homes, smart healthcare, intelligent vehicles, and smart cities. Section IV discusses NDN technology inclusively on the cloud, edge, VANET, and 5G. Section V delivers the conclusions and suggestions for future research.

II. NDN ARCHITECTURE, OPERATION, AND SERVICES

As a technology aimed at addressing the current Internet's limits, NDN offers a high-level architecture in which content moves from the origin of the content rather than the physical location. The future architecture of the Internet has shifted standards and repercussions due to many new applications and online services, appropriate mobility, sustainability, trustworthiness, and privacy. NDN is identified to meet the requirements of newly developed Internet applications [22]. NDN routers cache data with satisfied bandwidth [23]. NDN employs a hop-by-hop transmission method as an alternative to the usual paradigm. In this manner, NDN enables multicast and network-based caching features. Any node uses the gateway closest to the current route instead of the external server, saving data retrieval time. This considerably reduces redundancy traffic load throughout the network for the same content, significantly increasing overall network capacity.

A. ARCHITECTURE

The producer, consumer, and NDN router are the three main components of NDN. The producer is a service provider who distributes the content via NDN. Meanwhile, the consumer is a content subscriber who asks NDN for specific structures to fulfill user requests for the requested content, as described in Table 3: CS, PIT, and FIB. NDN retrieves content by name; naming schemes are application-specific and network-independent. A content name (CN) operates by accessing specific course content in its hierarchical structure. Fig 2 presents the standard OSI model with the NDN communication model. The NDN architecture has several key features:

1. **Named Data Objects**: NDN uses data-centric naming, where data is identified by its name instead of its location.
2. **Interest and Data Packets**: NDN uses Interest packets to request data and Data packets to return the requested data.
3. **Caching**: NDN allows intermediate nodes to cache data, reducing network congestion and improving data retrieval times.
4. **Security:** NDN uses digital signatures and encryption to provide data integrity and confidentiality.
5. **Routing**: NDN uses a combination of name prefix-based routing and in-network caching to forward Interest packets to their destinations.

These features make NDN well-suited for applications that require secure, scalable, and flexible data retrieval, such as content delivery, IoT, and vehicular networks.

B. OPERATION

In an NDN operation, the consumer initiates NDN communication by sending an Interest packet. Once the Interest packet grasps the producer, it will return with a Data packet. CN integrates into content, while the Data packet trails the route to ensure it to sent back to the consumer. The linked CN checks the CS for a match when a consumer Interest packet reaches the NDN router. Suppose related content finds, the NDN router handovers it through a Data packet allotted by the producer. The incoming interface for Interest packets adds an Interest aggregation process to the interface list. Consequently, the corresponding Data packet is available, and all attracted consumers accept a copy. If no PIT record exists for an inbound Interest packet, its route to FIB for the longest prefix match (LPM) for a CN.

When a corresponding FIB access this LPMs location, it routes to the relevant next-hop and forms a new PIT entry with its incoming interface. In contrast, a Data packet access to the NDN router searches all PIT records for a matching CN. All of the interfaces listed route the Data packet from the incoming interfaces. Subsequent PIT entry removes, and the content is kept in CS per the local caching policy to serve future requests. The Data packet is lost if there is no matching PIT entry. The operating procedure for the NDN router, represented in Fig 3, indicates that the requestor is looking for the content provided by the producer. Producer yield the content request from the consumer. When the NDN router receives such a request, first check CS to see if the required content is stored locally. The router uses the CN to search for PIT if a connected entry indicates that the NDN router keeps the content locally and sends it based on the subsequent PIT entry.

C. ROUTING

NDN packets are routed and forwarded using names. Consequently, contrasted with the IP architecture, NDN doesn't have addressing issues. No address fatigue issue with the NDN namespace. The routing strategy doesn't involve public and private addressing, and there is no use for Network Address Translation (NAT). There are three types of NDN routing, such as Distance Vector Routing (DVR) [24], Geographical Routing (GR) [25], and Link State Routing (LSR) [26].

In NDN GR routing, packets are delivered to the neighbor if the node does not have a neighbor closer to the destination. The LSR technique seeks the optimal global path in difference towards NDN GR routing. LSR picks all routing information before reach to the producer. Consequently, in LSR routing, each router delivers the data for all potential networks.

TABLE 3. NDN architecture and functionality.

Feature	Description
Content Store(CS)	Each Data packet is used by several consumers, for example, multiple individuals reading the same newspaper. NDN router caches a copy of the Data packet going through them in the CS until it replaces by new material. Exact matching of namesused to search CS entries.
Pending Interest Table (PIT)	PIT keeps an entry for each incoming Interest packet until its corresponding Data packet arrives or until the entry lifetime expires, whichever comes first. These PIT entries are accountable for transmitting Data packets to the consumer. PIT entries are searched by exact name matching.
Forwarding Information Base (FIB)	For every name prefix that can be reached, FIB keeps track of the next hop(s) and other relevant data. The routing protocol populates the FIB, which routes the Interest packet upstream

Another category in NDN routing is proactive routing and [27] reactive routing [28]. Proactive routing uses the router to gather all the information and saves the content into the NDN network. Each node in NDN routing uses the network information before updating the FIB to calculate paths. On-demand routing algorithms based on reactive protocols construct a path for a given destination. Once a path establishes, the node maintains it until it is no longer reachable. FIB in reactive routing neither function as the requesting nor the intermediary node.

Kuai et al. presented a cluster-based routing (CBR) protocol using clustering algorithms for picking cluster heads on alternate paths for information-centric wireless sensor networks (ICWSN) [29]. However, this strategy has significantly increased network lifetime and energy savings and does not rely on caching strategies. Other research has developed a strategy called SCaN-Mob to solve problems handover of producers in wireless networks. It provides a method for a cache replacement strategy and interest forwarding [30].

D. CACHING

Content caching at the NDN router, also known as in-network storage, is critical for supporting the primary notion of NDN's content-centric, with low cost suitable for peer-to-peer data distribution paradigm. In NDN, caching provides numerous advantages. Some advantages are that producer content supports truly separating content from other producers. It eradicates a single point of failure and decreases producer costs by

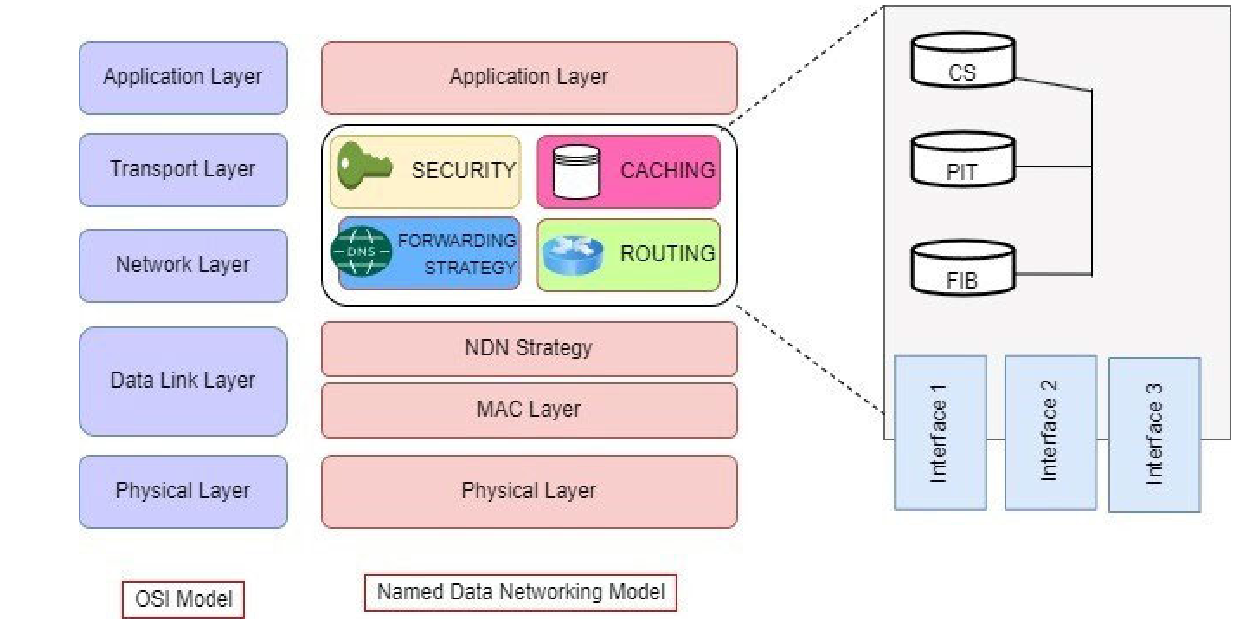

FIGURE 2. Comparison of OSI and NDN communication model.

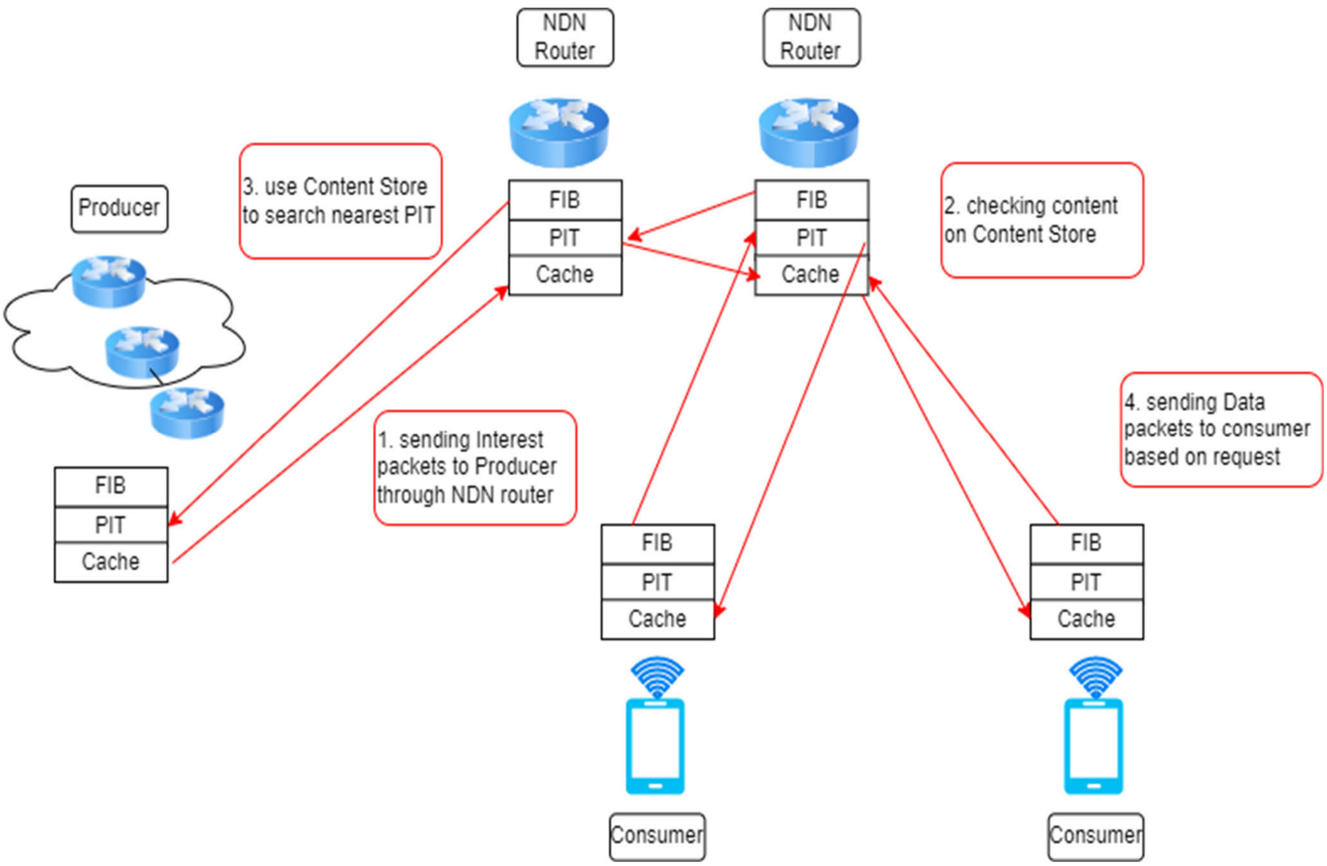

FIGURE 3. Standard NDN operations and services.

making several copies of the same material available in the NDN network [31]. Due to packet loss, it offers significant advantages to dynamic material in multicast or retransmission. It also reduces network strain and data propagation latency. Cache performance is often measured using the average number of hops, traversed content retrieval delay, and hit ratio. Propagation speed, measured in the time necessary to distribute content to the network core, is another relevant caching performance parameter. Data packet caches in the intermediate routers decide by using the caching policy. Consequently, caching strategies divide into cache placement and cache replacement.

E. FORWARDING STRATEGY

NDN uses a stateful forwarding plan to determine which mobile consumers are behind the traffic. NDN is a consumer-driven infrastructure. NDN forwarding techniques (FT) are another feature of NDN. It is a selective broadcast-based forwarding system that can make forwarding decisions based on past hit rate data. A lightweight forwarding technique compatible with IEEE802.15.4 technology [32]. It works with standard transmission NDN, not vehicular transmission. Vehicle communication has also made use of FT. A study has developed a better system for forwarding interest and data packets. It's called "data-based forwarding." Data packets are distributed based on how many nodes are in the content-based named network.

Unlike distance-based packet broadcasting, a researcher offered novel strategy techniques that analyze nodes' content worries and forward interest in the direction of more significant concern [33]. Another forwarding strategy solution is a new protocol for transferring named data in VANETs. The forwarding methods make it easier to spread interest and find data with unique names [34]. Mobility info of the vehicles in the neighboring database uses to choose the consumer's next-hop forwarders [35]. It offers a sophisticated NDN forwarding that keeps track of personal and nearby PITs to manage data and interest packets. This work also develops a periodic interest-generating mechanism to make nearby nodes aware of a neighboring node's PIT.

F. SECURITY

The critical problems in NDN are architectural security, cost-effective operations, security management, trust management, and confidentiality protection [36]. To facilitate access control and confidentiality, NDN employs content encryption. However, no reliable servers are required to apply security restrictions. Furthermore, the decryption key does not need to distribute because it delivers directly to the consumer. Only the private key can decrypt content encrypted with the public key. There are two types of NDN security encryption, asymmetric and symmetric. For symmetric encryption, by using symmetric keys, a secret key that retrieves from a signed Interest packet is required. A data producer can validate the consumer by marking it and returning an encrypted private key using the consumer's public key. Hao and Wang developed a solution for asymmetric encryption by integrating lightweight physical layer identity [37]. This method increases the differentiation rate and correct authentication probability for NDN security issues on the monitoring plane. Work in [38], a monitoring system for detecting anomalies using Bayesian Network. The last invasion comes from Ko and Mambo [39], which proposes Public Key Encryption Keyword Search (PEKS) for forwarding packets. It has overcome the issue of the cryptographic operation.

III. NDN APPLICATIONS

According to recent research, NDN applications are able to support users' emerging needs and requirements. Intelligent vehicles, smart cities, smart healthcare, and smart homes are the current NDN applications, as shown in Fig 4. The NDN application provides enormous benefits to human life through its enabled services. There are much research related to NDN application, as shown in Table 4. The most popular NDN application is the smart vehicles, followed by IoT applications, while the entertainment sector provides video. NDN also supports other categories, such as innovative environment and education.

Among the NDN applications used in smart vehicles are smart parking, intelligent entertainment, autonomous assistance, sensor systems, and route location identifiers, as shown in Table 5. NDN application that uses IoT has highlighted the interest of researchers, academicians, and industry players. For smart healthcare, the evolution of NDN application technology resulted in numerous advantages for patient happiness and gratification [40]. Wireless body area networks (WBAN) or RFID used in wearable devices that communicate with cloud computing are examples of NDN that use IoT technology in healthcare [41]. These devices provide an appealing alternative for mobile applications and monitoring systems, including blood pressure, ECG, and oxygen saturation [42]. Other healthcare applications include adversative drug reaction monitoring, diabetes prevention rehabilitation systems, inventory, medicine, and wheelchair management systems. IoT devices in NDN applications permit surgeons to observe patient health remotely.

NDN application also mainly report on multimedia application such as video streaming and video conference. Implementing NDN in video streaming improves stable links and minimizes broken links during transmission [43]. Other NDN applications allow synchronized Network Time Protocol by implementing a structure of NDN Hybrid [44]. Besides that, climate or weather monitoring, smart agriculture, and smart farming, waste management are examples of NDN applications in the environmental sector. Waste management is a critical concern for researchers globally. Some countries confuse garbage collection and waste management, yet NDN has improved this solution by applying an intelligent waste management system. Other applications, such as climate monitoring, weather predictions, and smart agriculture, produce more products at a lower cost. Using NDN technology, smart cities may provide intelligent industries, smart facilities to people, and smart homes [45]. This placement uses smart tools and applications for the environment, building more accessible healthcare and transportation. Citizens' smart digital ID is another feature that has many functions and uses. Fig 5 shows how NDN apps use IoT devices to administer, automate control, maintain buildings and factories, and monitor.

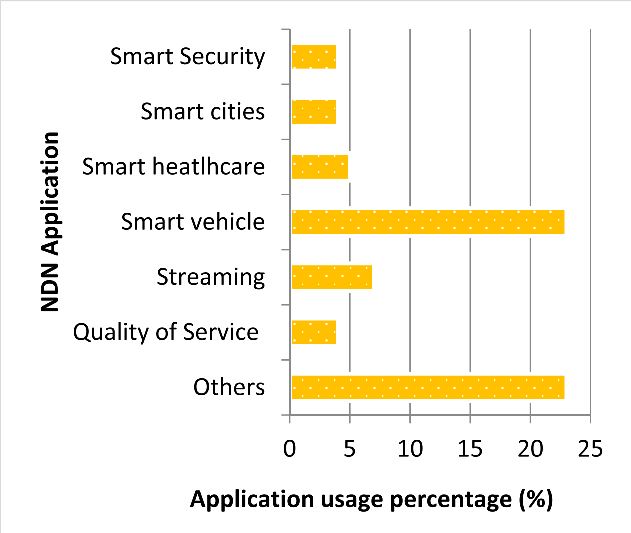

FIGURE 4. The trend of NDN applications.

It operates in many industries, including food, where automatic systems can trace, monitor, and monitor the freshness of food along the supply chain to improve manufacturing and shipping.

IV. NDN TECHNOLOGY

Various technologies enable NDN communication. The most popular ones in NDN technology are IoT, followed by VANET, 5G, edge, and cloud computing, as shown in Fig 6. Microcontrollers, microprocessors, and network interfaces are part of IoT devices. The 5G technology covers mobile devices' telecommunication networks, while the VANET provides a control mechanism for moving vehicles, and for both, the NDN significantly supports better performance. As for edge computing, the NDN is preferred for data storage management support. Table 6 maps the most popular simulation tools used for NDN technologies research.

A. BLOCKCHAIN

Blockchain, known as ledger technology, improves security and enhances the NDN to catch the content. The use of blockchain technology ensures a secure and transparent transfer of data between vehicles and other road entities. The data can include traffic conditions, road conditions, vehicle maintenance information, and more. Applying a reputation-based mechanism Blockchain improve caching in Vehicle Named Data Network (VNDN) and enhance trust for content access through consumer [46]. The VNDN network aims to improve road safety, reduce traffic congestion and make driving more efficient. Another issue with VNDN is the current structure dependent on IP base transportation.

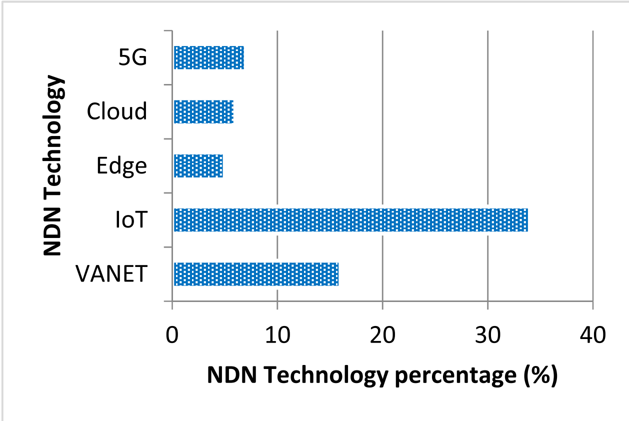

FIGURE 5. The trend review of NDN Technol.

Implementing Blockchain on NDN solves the issues and increases network security [47]. Other works have developed a new solution in VNDN by leveraging Blockchain and NDN [48]. This framework enhances the intelligent transportation system increasing trust and transparency. Secure data transmission needs to highlight, and a policy hiding scheme has come up with a solution for data revocation in VNDN [49]. Work in, [50] developed a reputation based on Blockchain to secure forwarding planes strategy. These techniques assure privacy and trust. Ahmad et al. [51] develop a solution by applying key management with a consensus algorithm to support privacy-aware on the VNDN network. Work in [52] proposes using key management based on blockchain technology to encounter mutual trust with anchors and improve verification efficiency.

Blockchain NDN (BoNDN) proposed by [53] supports broadcasting in NDN to generate blocks from subscriptions. Another solution to the NDN healthcare monitoring application issue solves by applying IoT blockchain technology. Fabric Hyperledger is used in work [54] to apply some functionality to security architecture on NDN.

Work in [55] covers Internet-of-Battlefield-Thing (IoBT) topics by applying Interest groups to overcome resource constraints. Distributed data management encounters security and privacy issues, and some problems solve by applying Blockchain. Work in [56] uses identifiers on Blockchain in the NDN environment to safely store the content. Alowish et al. came up with a survey on Blockchain over NDN that covers the benefit of Blockchain in decentralized payment, e-health care, and cloud computing [57].

B. CLOUD AND EDGE TECHNOLOGY

New-era research continues with VANET over cloud base technology. NDN came out with a unique solution called NDN-VC for a cloud-based that provides reliability and an intelligent transportation system [50]. Content priority causes issues in VNDN communication because the content is important before being transmitted. Thomas et al. propose a new algorithm that increases the hit ratio and reduces the

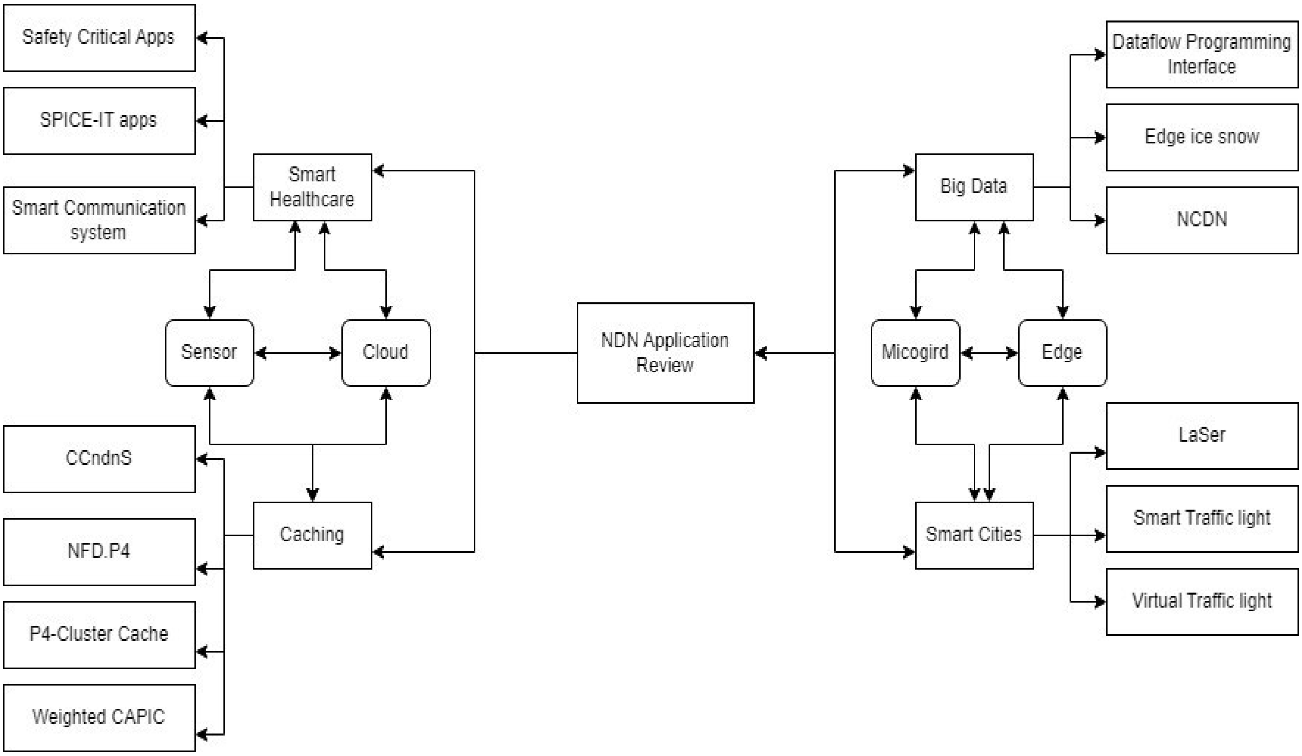

FIGURE 6. NDN application taxonomy.

TABLE 4. NDN applications research.

NDN Application	Year	Description
Lightweight Authentication and Secured Routing for NDN IoT (LaSer)	2018	scalable framework for NDN IoT lightweight authentication and hierarchical routing
Dataflow Programming Interface	2018	supply NDN transport techniques, which considerably enhances efficiency
Safety Critical Apps	2019	record and transmit raw sensor data to a home server capable of detecting critical healthcare occurrences
Smart Traffic Light	2019	eliminates traffic congestion
Content Caching strategy for NDN with Skip (CCndnS)	2020	caching policy for breaking cache dependency
Virtual Traffic Light	2020	assist pedestrians in safely passing across junctions without real traffic lights
Edge Ice Snow	2021	Enhance efficient computing
SPICE-IT Apps	2021	Autonomous indoor monitoring with a reporting mechanism that records violations on servers
Node-Failure Resilient CDN Solution (NCDN)	2021	using location-independent storage, provide resilience against node failure
Caching Algorithm (Weighted CAPIC)	2022	determine the link between the weight of the class and the cache hit ratio
Smart Communication System	2022	based on its residual energy level and a sleep mode scheduling algorithm determines the next hop forwarder
NDN In-Networking Cache Implementation Scheme with P4 (NFD. P4)	2022	replace the programmable switch's memory space.

signal overhead compared to IP architecture [58]. The latest discussion on NDN cloud is application distribution and network architecture. Work in [59] uses Geographical Vehicular Central Data Networking (GeoVCDN) to distribute vehicle content and improve efficiency compared to rendezvous and initial NDN networks. Macrovehicular cloud comes with an

TABLE 5. Major classification for NDN application.

Major Classification	Reference	Description	Technology
Transportation system	[46][47][48][49][50][51][52][56][57][58][61][62][63][64][65][67][68][69][70][71][72][73]	• Filter and rank IoT traffic and permit delay-tolerant, latency apps to access data efficiently. • Categorize the cyberattack hitches for vehicular CPS (VCPS) and NDN-based cyber-resilient meet and the integrated architecture for VCPS. • Timely answer to the vehicle's data inquiry. • Optimize the content request mechanism also lessen the broadcast storm issues. • Create a hierarchical router topology and a hierarchical data/interest namespace. • Improves cluster formation stability, allowing for effective content retrieval through V2V communications. • Improve service performance, such as minimizing data acquisition time, and develop a data caching strategy that considers the spatial-temporal features of data.	Technology – VANET, FANET, Cloud, SDN, SDVN Ad-hoc Network
Internet of Things	[32][37][70][71][72][73] [74][75][76]	• NDN is incorporating the lightweight and unforgeable PHY-I for NDN signature method for MEC- NDN-IoT. • Integrate NDN with ECC to obtain rapid information response time. • NDN over IEEE 802.15.4 requires a lightweight forwarding approach. • The package-level security mechanism includes a data package authentication system. • CPA preservation using a certificate-less signature technique in NDN-based IoT networks. • NDN using NDN content caching mechanism as a springboard for novel Endpoint Linked Green Content Caching technique to decrease energy usage in NDN-based IoT topology. • Data availability needs to be jeopardized by increased IoT network dynamics associated with sensor mobility.	Technology - VANET, 5G, VR
Streaming	[43][44][[77]][78][79][80]	• The NTP pool project has issues in the context of the NTP and one of its most extensively utilized deployments for NTP server discovery. • It explains the background, elaborates the key concepts, and presents the academic video lectures that use the most recent advancements in the NDN methodology and its applications. • To offer a smart QoE-aware ABR, a variety strategy that merges hybrid technology with in-network Caching mechanisms. • Utilizes the small cell idea and the deployment of wireless backhauls, inspired by the many features and performance of the LTE advanced network.	Technology – IoT, 5G, Online presentation

TABLE 6. Simulation tools for NDN technology research.

Technology	Paper	Method	Tools
IoT	[80][81][82][83][84][85] [86][87][88][89][90]	Experiment, mathematical model, security analysis	ns-3, NDN SIM, Automated Validation of Internet Security Protocols and Applications (AVISPA)
VANET	[91][92][93][94][95][96] [97][98][99][100][101] [102][103][104][105][106]	Experiments, mathematical model, machine learning	ns-3, NDN SIM
5G	[107][108][109][77][110][111][112]	Experiments, trapdoor technology, machine learning	ns-3, NDN SIM
Cloud and Edge	[105][113][114][115] [116][60][117]	Real experiment, mathematical model.	NDN SIM, omnet
Blockchain	[118][53][119][55][120][121][122]	Real experiments and mathematical model	ns-3, omnet, opnet
AI	[123][124][125][126] [127][128]	Experiments and machine learning	NDN SIM, opnet

issue of reverse data disruption and data cost. NDN-based aVC framework (NVCF) improves data acquisition and content transmission success [60].

NDN over-edge cloud computing (ECC) gives many benefits in terms of security, flexibility, and resiliency. Work in [61], hybrid NDN over ECC gives a higher response time than traditional edge computing.

Other work in edge computing integrates with IoT applications. One research found that the previous Internet of Things Cloud (IoTC) improved data retrieval based on IP architecture, but it's hard to embed IP addressing on IoT technology. Based on IoT, NDN proposes to overcome IP addressing issues, improve data efficiency by almost 9 percent, and reduce the cost to 42 percent compared to the traditional IoT approach. Other solutions also give better results to reduce cost and increase data retrieval by integrating virtual cloud and NDN [62].

C. ARTIFICIAL INTELLIGENCE

To establish a value-oriented ecosystem, upgrading from IP-based to knowledge-driven improves NDN technology significantly. Digital tokenization enhances storage, computing, and networking by embedding blockchain technology [63]. In edge computing, lack of content identifiers but more on host-centric communication urge toward NDN AI. NDN has developed a solution for edge computing by implementing a machine algorithm suited for user-centric communication [64]. Edge computing is constantly issuing big data and cloud computing issues. NDN AI evolution comes with a solution in edge computing that resolves big input data and reduces delay latency [65]. NDN AI also comes with a solution to enhance security and stability routing. A collusive Interest Flooding Attack (CIFA) is a vulnerable attack that affects producers to respond with malicious Interest packets. By applying NCIFA [66], overcome security issues on NDN traffic.

D. INTERNET OF THINGS

IoT uses 802.15.4 protocol to communicate at a satisfactory rate, increase data range and reduce the level of energy. To enable integration of IoT device IoT protocol communication such as 6lowPAN, NDN is the alternative to resolve mobility, and content is human-readable. A solution with Mr-IoT to control access to billion data on the NDN network [67]. Smart agriculture is one solution that uses NDN over IoT to reduce energy consumption and cost overhead [68]. Touati et al. find that in IoT, billions of data reproduce every single time. It solves the issue of dynamic computing for content delivery, managing high-volume data traffic and service response time [69]. Table 6 shows the summary of simulation tools of NDN technology research.

V. CONCLUSION

This manuscript provides a concise explanation of NDN's architecture, operation, and services, as well as the most recent technological development and application. Bringing to light the most current, being the primary area of concentration and widely researched NDN technology, is the Internet of Things. Other fields, such as Artificial Intelligence, Blockchain, and Cloud-Edge, are also receiving a lot of interest from researchers. In the meantime, in descending order, the NDN applications sector that is the most popular is the transportation sector, followed by the Internet of Things sector, the streaming sector, and finally, the healthcare sector. Eventually, to be more specific, the smart vehicle, smart healthcare, and smart city categories are considered to be the subfields of application within the sectors.

REFERENCES

[1] S. A. Gbadamosi, G. P. Hancke, and A. M. Abu-Mahfouz, "Building upon NB-IoT networks: A roadmap towards 5G new radio networks," *IEEE Access*, vol. 8, pp. 188641–188672, 2020, doi: 10.1109/ACCESS.2020.3030653.

[2] A. H. M. Aman, W. H. Hassan, S. Sameen, Z. S. Attarbashi, M. Alizadeh, and L. A. Latiff, "IoMT amid COVID-19 pandemic: Application, architecture, technology, and security," *J. Netw. Comput. Appl.*, vol. 174, Jan. 2021, Art. no. 102886, doi: 10.1016/j.jnca.2020.102886.

[3] A. H. M. Aman, E. Yadegaridehkordi, Z. S. Attarbashi, R. Hassan, and Y.-J. Park, "A survey on trend and classification of Internet of Things reviews," *IEEE Access*, vol. 8, pp. 111763–111782, 2020, doi: 10.1109/ACCESS.2020.3002932.

[4] W. M. H. Azamuddin, A. H. M. Aman, R. Hassan, and T. A. N. Abdali, "Named data networking mobility: A survey," in *Proc. Int. Conf. Emerg. Technol. Trends Internet Things Comput.*, vol. 1548. Cham, Switzerland: Springer, 2022, pp. 266–281.

[5] F. A. Karim, A. H. M. Aman, R. Hassan, K. Nisar, and M. Uddin, "Named data networking: A survey on routing strategies," *IEEE Access*, vol. 10, pp. 90254–90270, 2022, doi: 10.1109/ACCESS.2022.3201083.

[6] A. Aboodi, T.-C. Wan, and G.-C. Sodhy, "Survey on the incorporation of NDN/CCN in IoT," *IEEE Access*, vol. 7, pp. 71827–71858, 2019, doi: 10.1109/ACCESS.2019.2919534.

[7] IEEE. (2021). *IEEE Access: The Multidisciplinary Open Access Journal*. Accessed: Mar. 21, 2021. [Online]. Available: https://ieeeaccess.ieee.org/

[8] (2021). *ScienceDirect*. Accessed: Mar. 21, 2021. [Online]. Available: https://www.sciencedirect.com/

[9] RFC Series Editor. (2018). *IETF|RFCs*. [Online]. Available: https://ietf.org/standards/rfcs/%0Ahttps://www.ietf.org/standards/rfcs/

[10] Google. (2021). *Google Shcolar*. Accessed: Mar. 21, 2021. [Online]. Available: https://scholar.google.com/

[11] A. Benarfa, M. Hassan, E. Losiouk, A. Compagno, M. B. Yagoubi, and M. Conti, "ChoKIFA+: An early detection and mitigation approach against interest flooding attacks in NDN," *Int. J. Inf. Secur.*, vol. 20, no. 3, pp. 269–285, Jun. 2021, doi: 10.1007/s10207-020-00500-z.

[12] Z. Zhang, Y. Yu, H. Zhang, E. Newberry, S. Mastorakis, Y. Li, A. Afanasyev, and L. Zhang, "An overview of security support in named data networking," *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 62–68, Nov. 2018, doi: 10.1109/MCOM.2018.1701147.

[13] Z. Li, Y. Xu, B. Zhang, L. Yan, and K. Liu, "Packet forwarding in named data networking requirements and survey of solutions," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1950–1987, 2nd Quart., 2019, doi: 10.1109/COMST.2018.2880444.

[14] S. Nayak, R. Patgiri, and A. Borah, "A survey on the roles of Bloom filter in implementation of the named data networking," *Comput. Netw.*, vol. 196, Sep. 2021, Art. no. 108232, doi: 10.1016/j.comnet.2021.108232.

[15] B. Rainer and S. Petscharnig, "Challenges and opportunities of named data networking in vehicle-to-everything communication: A review," *Information*, vol. 9, no. 11, pp. 1–19, 2018, doi: 10.3390/info9110264.

[16] C. Chen, C. Wang, T. Qiu, M. Atiquzzaman, and D. O. Wu, "Caching in vehicular named data networking: Architecture, schemes and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2378–2407, 4th Quart., 2020, doi: 10.1109/COMST.2020.3005361.

[17] H. Khelifi, S. Luo, B. Nour, H. Moungla, Y. Faheem, R. Hussain, and A. Ksentini, "Named data networking in vehicular ad hoc networks: State-of-the-art and challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 320–351, 1st Quart., 2020, doi: 10.1109/COMST.2019.2894816.

[18] H. Al-Omaisi, E. A. Sundararajan, R. Alsaqour, N. F. Abdullah, and M. Abdelhaq, "A survey of data dissemination schemes in vehicular named data networking," *Veh. Commun.*, vol. 30, Aug. 2021, Art. no. 100353, doi: 10.1016/j.vehcom.2021.100353.

[19] A. Suwannasa, M. Broadbent, and A. Mauthe, "Effectiveness of vicinity-based content finding in mobile NDN environments," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2021, pp. 343–348, doi: 10.1109/ICOIN50884.2021.9333948.

[20] K. K. Singh and R. K. Dudeja, "Hybrid information placement in named data networking-Internet of Things system," in *Proc. 8th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Mar. 2022, pp. 593–601, doi: 10.1109/ICACCS54159.2022.9785184.

[21] M. A. Naeem, T. N. Nguyen, R. Ali, K. Cengiz, Y. Meng, and T. Khurshaid, "Hybrid cache management in IoT-based named data networking," *IEEE Internet Things J.*, vol. 9, no. 10, pp. 7140–7150, May 2022, doi: 10.1109/JIOT.2021.3075317.

[22] B. S. Paris, "Time constructs: Design ideology and a future internet," *Time Soc.*, vol. 30, no. 1, pp. 126–149, Feb. 2021, doi: 10.1177/0961463X20985316.

[23] A. Detti, L. Bracciale, P. Loreti, G. Rossi, and N. B. Melazzi, "A cluster-based scalable router for information centric networks," *Comput. Netw.*, vol. 142, pp. 24–32, Sep. 2018, doi: 10.1016/j.comnet.2018.06.003.

[24] I. V. S. Brito, "NDVR: NDN distance vector routing," 2021, *arXiv:2102.13584*.

[25] B. Aldahlan and Z. Fei, "A geographic routing strategy with DTN support for vehicular named data networking," in *Proc. 22nd IEEE Int. Conf. Comput. Sci. Eng. 17th IEEE Int. Conf. Embedded Ubiquitous Comput.*, Aug. 2019, pp. 361–366, doi: 10.1109/CSE/EUC.2019.00075.

[26] L. Wang, V. Lehman, A. K. M. M. Hoque, B. Zhang, Y. Yu, and L. Zhang, "A secure link state routing protocol for NDN," *IEEE Access*, vol. 6, pp. 10470–10482, 2018, doi: 10.1109/ACCESS.2017.2789330.

[27] M. B. Lehmann, M. P. Barcellos, and A. Mauthe, "Providing producer mobility support in NDN through proactive data replication," in *Proc. NOMS-IEEE/IFIP Netw. Oper. Manage. Symp.*, Apr. 2016, pp. 383–391, doi: 10.1109/NOMS.2016.7502835.

[28] B. Hammi, S. Zeadally, H. Labiod, R. Khatoun, Y. Begriche, and L. Khoukhi, "A secure multipath reactive protocol for routing in IoT and HANETs," *Ad Hoc Netw.*, vol. 103, Jun. 2020, Art. no. 102118, doi: 10.1016/j.adhoc.2020.102118.

[29] M. Kuai, X. Hong, and Q. Yu, "Delay-tolerant forwarding strategy for named data networking in vehicular environment," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 31, no. 1, pp. 1–12, 2019, doi: 10.1504/IJAHUC.2019.099634.

[30] F. R. C. Araújo, A. M. de Sousa, and L. N. Sampaio, "SCaN-Mob: An opportunistic caching strategy to support producer mobility in named data wireless networking," *Comput. Netw.*, vol. 156, pp. 62–74, Jun. 2019, doi: 10.1016/j.comnet.2019.04.008.

[31] C. Gündoğan, P. Kietzmann, T. C. Schmidt, and M. Wählisch, "Designing a LoWPAN convergence layer for the information centric Internet of Things," *Comput. Commun.*, vol. 164, pp. 114–123, Dec. 2020, doi: 10.1016/j.comcom.2020.10.002.

[32] A. Abane, M. Daoui, S. Bouzefrane, and P. Muhlethaler, "A lightweight forwarding strategy for named data networking in low-end IoT," *J. Netw. Comput. Appl.*, vol. 148, Dec. 2019, Art. no. 102445, doi: 10.1016/j.jnca.2019.102445.

[33] M. Alhowaidi, D. Nadig, B. Hu, B. Ramamurthy, and B. Bockelman, "Cache management for large data transfers and multipath forwarding strategies in named data networking," *Comput. Netw.*, vol. 199, Nov. 2021, Art. no. 108437, doi: 10.1016/j.comnet.2021.108437.

[34] Y. Xu, S. Tong, T. Zhang, W. Sun, X. Hu, and Q. Xiang, "COMPASS: Directing named data transmission in VANETs by dynamic directional interfaces," *IEEE Access*, vol. 8, pp. 8418–8435, 2020, doi: 10.1109/ACCESS.2019.2963547.

[35] J. Wang, J. Luo, J. Zhou, and Y. Ran, "A mobility-predict-based forwarding strategy in vehicular named data networks," in *Proc. IEEE Global Commun. Conf.*, Dec. 2020, pp. 1–6, doi: 10.1109/GLOBECOM42002.2020.9322164.

[36] T. Liu, M. Zhang, J. Zhu, R. Zheng, R. Liu, and Q. Wu, "ACCP: Adaptive congestion control protocol in named data networking based on deep learning," *Neural Comput. Appl.*, vol. 31, no. 9, pp. 4675–4683, Sep. 2019, doi: 10.1007/s00521-018-3408-2.

[37] P. Hao and X. Wang, "Integrating PHY security into NDN-IoT networks by exploiting MEC: Authentication efficiency, robustness, and accuracy enhancement," *IEEE Trans. Signal Inf. Process. over Netw.*, vol. 5, no. 4, pp. 792–806, Dec. 2019, doi: 10.1109/TSIPN.2019.2932678.

[38] H. L. Mai, T. Nguyen, G. Doyen, R. Cogranne, W. Mallouli, E. M. de Oca, and O. Festor, "Towards a security monitoring plane for named data networking and its application against content poisoning attack," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp.*, Apr. 2018, pp. 1–9, doi: 10.1109/NOMS.2018.8406246.

[39] K. T. Ko and M. Mambo, "Trapdoor assignment of PEKS-based NDN strategy in two-tier networks," in *Proc. 16th Int. Conf. Mobility, Sens. Netw. (MSN)*, Dec. 2020, pp. 607–613, doi: 10.1109/MSN50589.2020.00099.

[40] D. Saxena and V. Raychoudhury, "Design and verification of an NDN-based safety-critical application: A case study with smart healthcare," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 5, pp. 991–1005, May 2019, doi: 10.1109/TSMC.2017.2723843.

[41] W. M. H. Azamuddin, A. H. M. Aman, R. Hassan, and N. Mansor, "Comparison of named data networking mobility methodology in a merged cloud Internet of Things and artificial intelligence environment," *Sensors*, vol. 22, no. 17, p. 6668, Sep. 2022, doi: 10.3390/s22176668.

[42] S. S. Ullah, S. Hussain, A. Gumaei, and H. AlSalman, "A secure NDN framework for Internet of Things enabled healthcare," *Comput., Mater. Continua*, vol. 67, no. 1, pp. 223–240, 2021, doi: 10.32604/cmc.2021.014413.

[43] I. Dasgupta, S. Shannigrahi, and M. Zink, "A hybrid NDN-IP architecture for live video streaming: From host-based to content-based delivery to improve QoE," *Int. J. Semantic Comput.*, vol. 16, no. 2, pp. 163–187, Jun. 2022, doi: 10.1142/S1793351X22400074.

[44] A. Mtibaa and S. Mastorakis, "NDNTP: A named data networking time protocol," *IEEE Netw.*, vol. 34, no. 6, pp. 235–241, Nov. 2020, doi: 10.1109/MNET.011.2000169.

[45] T. Mick, R. Tourani, and S. Misra, "LASeR: Lightweight authentication and secured routing for NDN IoT in smart cities," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 755–764, Apr. 2018, doi: 10.1109/JIOT.2017.2725238.

[46] K. Lei, S. Zhong, F. Zhu, K. Xu, and H. Zhang, "An NDN IoT content distribution model with network coding enhanced forwarding strategy for 5G," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2725–2735, Jun. 2018, doi: 10.1109/TII.2017.2781372.

[47] S. Muralidharan, A. Roy, and N. Saxena, "MDP-IoT: MDP based interest forwarding for heterogeneous traffic in IoT-NDN environment," *Future Gener. Comput. Syst.*, vol. 79, pp. 892–908, Feb. 2018, doi: 10.1016/j.future.2017.08.058.

[48] S. H. Bouk, S. H. Ahmed, R. Hussain, and Y. Eun, "Named data Networking's intrinsic cyber-resilience for vehicular CPS," *IEEE Access*, vol. 6, pp. 60570–60585, 2018, doi: 10.1109/ACCESS.2018.2875890.

[49] E. Barka, C. Kerrache, R. Hussain, N. Lagraa, A. Lakas, and S. Bouk, "A trusted lightweight communication strategy for flying named data networking," *Sensors*, vol. 18, no. 8, p. 2683, Aug. 2018, doi: 10.3390/s18082683.

[50] R. Hussain, S. H. Bouk, N. Javaid, A. M. Khan, and J. Lee, "Realization of VANET-based cloud services through named data networking," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 168–175, Aug. 2018, doi: 10.1109/MCOM.2018.1700514.

[51] F. Ahmad, C. A. Kerrache, F. Kurugollu, and R. Hussain, "Realization of blockchain in named data networking-based Internet-of-Vehicles," *IT Prof.*, vol. 21, no. 4, pp. 41–47, Jul. 2019, doi: 10.1109/MITP.2019.2912142.

[52] M. Kuai and X. Hong, "Location-based deferred broadcast for ad-hoc named data networking," *Future Internet*, vol. 11, no. 6, p. 139, Jun. 2019, doi: 10.3390/FI11060139.

[53] J. Guo, M. Wang, B. Chen, S. Yu, H. Zhang, and Y. Zhang, "Enabling blockchain applications over named data networking," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 19–24, doi: 10.1109/ICC.2019.8761919.

[54] H. Yang, J. Yuan, H. Yao, Q. Yao, A. Yu, and J. Zhang, "Blockchain-based hierarchical trust networking for JointCloud," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1667–1677, Mar. 2020, doi: 10.1109/JIOT.2019.2961187.

[55] R. Doku, D. B. Rawat, M. Garuba, and L. Njilla, "Fusion of named data networking and blockchain for resilient Internet-of-Battlefield-Things," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2020, pp. 1–6, doi: 10.1109/CCNC46108.2020.9045395.

[56] E. Affum, X. Zhang, X. Wang, and J. B. Ansuura, "Efficient lattice CP-ABE AC scheme supporting reduced-OBDD structure for CCN/NDN," *Symmetry*, vol. 12, no. 1, p. 166, Jan. 2020, doi: 10.3390/SYM12010166.

[57] M. Alowish, Y. Shiraishi, Y. Takano, M. Mohri, and M. Morii, "Stabilized clustering enabled V2 V communication in an NDN-SDVN environment for content retrieval," *IEEE Access*, vol. 8, pp. 135138–135151, 2020, doi: 10.1109/ACCESS.2020.3010881.

[58] Y. Thomas, N. Fotiou, S. Toumpis, and G. C. Polyzos, "Improving mobile ad hoc networks using hybrid IP-information centric networking," *Comput. Commun.*, vol. 156, pp. 25–34, Apr. 2020, doi: 10.1016/j.comcom.2020.03.029.

[59] G. Wilhelm, H. Fouchal, and M. Ayaida, "Vehicular context cloud networking for intelligent transport systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6, doi: 10.1109/ICC40277.2020.9148859.

[60] X. Wang and S. Cai, "Named data networking-based macrovehicular cloud framework," *IEEE Syst. J.*, vol. 15, no. 4, pp. 5646–5653, Dec. 2021, doi: 10.1109/JSYST.2020.3017572.

[61] V. Sampath, S. Karthik, and R. Sabitha, "Position-based adaptive clustering model (PACM) for efficient data caching in vehicular named data networks (VNDN)," *Wireless Pers. Commun.*, vol. 117, no. 4, pp. 2955–2971, Apr. 2021, doi: 10.1007/s11277-020-07208-2.

[62] C. Gundogan, P. Kietzmann, M. S. Lenders, H. Petersen, M. Frey, T. C. Schmidt, F. Shzu-Juraschek, and M. Wahlisch, "The impact of networking protocols on massive M2M communication in the industrial IoT," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 4, pp. 4814–4828, Dec. 2021, doi: 10.1109/TNSM.2021.3089549.

[63] C. Chen, J. Jiang, R. Fu, L. Chen, C. Li, and S. Wan, "An intelligent caching strategy considering time-space characteristics in vehicular named data networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 19655–19667, Oct. 2022, doi: 10.1109/TITS.2021.3128012.

[64] Q. T. Thai, N. Ko, S. H. Byun, and S.-M. Kim, "Design and implementation of NDN-based ethereum blockchain," *J. Netw. Comput. Appl.*, vol. 200, Apr. 2022, Art. no. 103329, doi: 10.1016/j.jnca.2021.103329.

[65] W. U. I. Zafar, M. A. U. Rehman, F. Jabeen, S. Ghouzali, Z. Rehman, and W. Abdul, "Context-aware pending interest table management scheme for NDN-based VANETs," *Sensors*, vol. 22, no. 11, p. 4189, May 2022, doi: 10.3390/s22114189.

[66] R.-T. Lee, Y.-B. Leau, Y.-J. Park, and J. H. Obit, "A perspective towards NCIFA and CIFA in named-data networking architecture," in *Computational Science and Technology* (Lecture Notes in Electrical Engineering), vol. 603, R. Alfred, Y. Lim, H. Haviluddin, and C. K. On, Eds. Singapore: Springer, Aug. 2020, pp. 481–490.

[67] J. Sun, "Certificateless batch authentication scheme and intrusion detection model based on the mobile edge computing technology NDN-IoT environment," *J. Function Spaces*, vol. 2022, pp. 1–9, Jul. 2022, doi: 10.1155/2022/5926792.

[68] R. A. Al-Share, A. S. Shatnawi, and B. Al-Duwairi, "Detecting and mitigating collusive interest flooding attacks in named data networking," *IEEE Access*, vol. 10, pp. 65996–66017, 2022, doi: 10.1109/ACCESS.2022.3184304.

[69] H. Touati, A. Aboud, and B. Hnich, "Named data networking-based communication model for Internet of Things using energy aware forwarding strategy and smart sleep mode," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 3, p. e6584, Feb. 2022, doi: 10.1002/cpe.6584.

[70] H. Huang, Y. Wu, F. Xiao, and R. Malekian, "An efficient signature scheme based on mobile edge computing in the NDN-IoT environment," *IEEE Trans. Computat. Social Syst.*, vol. 8, no. 5, pp. 1108–1120, Oct. 2021, doi: 10.1109/TCSS.2021.3076209.

[71] S. Hussain, S. S. Ullah, A. Gumaei, M. Al-Rakhami, I. Ahmad, and S. M. Arif, "A novel efficient certificateless signature scheme for the prevention of content poisoning attack in named data networking-based Internet of Things," *IEEE Access*, vol. 9, pp. 40198–40215, 2021, doi: 10.1109/ACCESS.2021.3063490.

[72] A. Kaci and A. Rachedi, "Named data networking architecture for Internet of Vehicles in the era of 5G," *Ann. Telecommun.*, vol. 76, nos. 9–10, pp. 717–729, Oct. 2021, doi: 10.1007/s12243-021-00866-8.

[73] O. Karrakchou, N. Samaan, and A. Karmouch, "Mapping applications intents to programmable NDN data-planes via event-B machines," *IEEE Access*, vol. 10, pp. 29668–29686, 2022, doi: 10.1109/ACCESS.2022.3158753.

[74] R. Ullah, M. A. U. Rehman, and B.-S. Kim, "Design and implementation of an open source framework and prototype for named data networking-based edge cloud computing system," *IEEE Access*, vol. 7, pp. 57741–57759, 2019, doi: 10.1109/ACCESS.2019.2914067.

[75] H. S. Shrisha and U. Boregowda, "An energy efficient and scalable endpoint linked green content caching for named data network based Internet of Things," *Results Eng.*, vol. 13, Mar. 2022, Art. no. 100345, doi: 10.1016/j.rineng.2022.100345.

[76] X. Qian and X. Wang, "Content-centric IoT-based air pollution monitoring," *Wireless Pers. Commun.*, vol. 123, no. 4, pp. 3213–3222, Apr. 2022, doi: 10.1007/s11277-021-09284-4.

[77] M. Meddeb, A. Dhraief, A. Belghith, T. Monteil, K. Drira, and S. Gannouni, "AFIRM: Adaptive forwarding based link recovery for mobility support in NDN/IoT networks," *Future Gener. Comput. Syst.*, vol. 87, pp. 351–363, Oct. 2018, doi: 10.1016/j.future.2018.04.087.

[78] V. P. Singh and R. L. Ujjwal, “A walkthrough of name data networking: Architecture, functionalities, operations and open issues,” *Sustain. Comput., Informat. Syst.*, vol. 28, Dec. 2020, Art. no. 100419, doi: 10.1016/j.suscom.2020.100419.

[79] D. Kanellopoulos, “Academic video lectures over named data networking,” *Inf. Discovery Del.*, vol. 48, no. 4, pp. 165–177, Mar. 2020, doi: 10.1108/IDD-10-2019-0071.

[80] Y. Hayamizu, K. Goto, M. Bandai, and M. Yamamoto, “QoE-aware bitrate selection in cooperation with in-network caching for information-centric networking,” *IEEE Access*, vol. 9, pp. 165059–165071, 2021, doi: 10.1109/ACCESS.2021.3133851.

[81] M. Almutiq, L. Sellami, and B. Alaya, “Dynamic vehicular clustering enhancing video on demand services over vehicular ad-hoc networks,” *Comput., Mater. Continua*, vol. 72, no. 2, pp. 3493–3510, 2022, doi: 10.32604/cmc.2022.024571.

[82] H. Cao, S. Liu, L. Wu, and Z. Guan, “SCRAPPOR: An efficient privacy-preserving algorithm base on sparse coding for information-centric IoT,” *IEEE Access*, vol. 6, pp. 63143–63154, 2018, doi: 10.1109/ACCESS.2018.2876707.

[83] A. Abane, M. Daoui, S. Bouzefrane, and P. Muhlethaler, “NDN-over-ZigBee: A ZigBee support for named data networking,” *Future Gener. Comput. Syst.*, vol. 93, pp. 792–798, Apr. 2019, doi: 10.1016/j.future.2017.09.053.

[84] M. Amadeo, G. Ruggeri, C. Campolo, A. Molinaro, V. Loscrí, and C. T. Calafate, “Fog computing in IoT smart environments via named data networking: A study on service orchestration mechanisms,” *Future Internet*, vol. 11, no. 11, p. 222, Oct. 2019, doi: 10.3390/fi11110222.

[85] M. Rezazad and Y. C. Tay, “Decoupling NDN caches via CCndnS: Design, analysis, and application,” *Comput. Commun.*, vol. 151, pp. 338–354, Feb. 2020, doi: 10.1016/j.comcom.2019.12.053.

[86] L. Gameiro, C. Senna, and M. Luís, “NdnIoT-FC: IoT devices as first-class traffic in name data networks,” *Future Internet*, vol. 12, no. 11, p. 207, Nov. 2020, doi: 10.3390/fi12110207.

[87] M. Rehman, H. Khattak, A. S. Alzahrani, I. Ullah, M. Adnan, S. S. Ullah, N. U. Amin, S. Hussain, and S. J. Khattak, “A lightweight nature heterogeneous generalized signcryption (HGSC) scheme for named data networking-enabled Internet of Things,” *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–20, Nov. 2020, doi: 10.1155/2020/8857272.

[88] M. Rahouti, K. Xiong, and Y. Xin, “Secure software-defined networking communication systems for smart cities: Current status, challenges, and trends,” *IEEE Access*, vol. 9, pp. 12083–12113, 2021, doi: 10.1109/ACCESS.2020.3047996.

[89] Q. Wang, B. Lee, N. Murray, and Y. Qiao, “MR-IoT: An information centric MapReduce framework for IoT,” in *Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2018, pp. 1–6, doi: 10.1109/CCNC.2018.8319184.

[90] M. Amadeo, C. Campolo, A. Molinaro, and G. Ruggeri, “IoT data processing at the edge with named data networking,” in *Proc. 24th Eur. Wireless Conf.*, 2018, pp. 38–43.

[91] N. Yang, K. Chen, and M. Wang, “SmartDetour: Defending blackhole and content poisoning attacks in IoT NDN networks,” *IEEE Internet Things J.*, vol. 8, no. 15, pp. 12119–12136, Aug. 2021, doi: 10.1109/JIOT.2021.3061531.

[92] M. T. R. Khan, M. M. Saad, M. A. Tariq, J. Akram, and D. Kim, “SPICE-IT: Smart COVID-19 pandemic controlled eradication over NDN-IoT,” *Inf. Fusion*, vol. 74, pp. 50–64, Oct. 2021, doi: 10.1016/j.inffus.2021.03.005.

[93] S. Hussain, S. S. Ullah, and I. Ali, “An efficient content source verification scheme for multi-receiver in NDN-based Internet of Things,” *Cluster Comput.*, vol. 25, no. 3, pp. 1749–1764, Jun. 2022, doi: 10.1007/s10586-021-03384-3.

[94] S. Alduayji, A. Belghith, A. Gazdar, and S. Al-Ahmadi, “PF-ClusterCache: Popularity and freshness-aware collaborative cache clustering for named data networking of things,” *Appl. Sci.*, vol. 12, no. 13, p. 6706, Jul. 2022, doi: 10.3390/app12136706.

[95] S. V. V. Karthik and J. A. V. Selvi, “Hybrid cluster made content forwarding and light weight sign encryption IoT based named data network using African buffalo optimization algorithm,” *J. Intell. Fuzzy Syst.*, vol. 43, no. 3, pp. 2891–2905, Jul. 2022, doi: 10.3233/JIFS-212674.

[96] S. Sharma and A. Kaul, “VANETs cloud: Architecture, applications, challenges, and issues,” *Arch. Comput. Methods Eng.*, vol. 28, no. 4, pp. 2081–2102, Jun. 2021, doi: 10.1007/s11831-020-09447-9.

[97] C. Gundogan, C. Amsuss, T. C. Schmidt, and M. Wahlisch, “Content object security in the Internet of Things: Challenges, prospects, and emerging solutions,” *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 1, pp. 538–553, Mar. 2022, doi: 10.1109/TNSM.2021.3099902.

[98] R. K. Dudeja, R. S. Bali, and G. S. Aujla, “Secure and pervasive communication framework using named data networking for connected healthcare,” *Comput. Electr. Eng.*, vol. 100, May 2022, Art. no. 107806, doi: 10.1016/j.compeleceng.2022.107806.

[99] Z. Zhang, T. Yu, X. Ma, Y. Guan, P. Moll, and L. Zhang, “Sovereign: Self-contained smart home with data-centric network and security,” *IEEE Internet Things J.*, vol. 9, no. 15, pp. 13808–13822, Aug. 2022, doi: 10.1109/JIOT.2022.3144980.

[100] P.-H. Tsai, J.-B. Zhang, and M.-H. Tsai, “An efficient probe-based routing for content-centric networking,” *Sensors*, vol. 22, no. 1, p. 341, Jan. 2022, doi: 10.3390/s22010341.

[101] H. Khelifi, S. Luo, B. Nour, H. Moungla, and S. H. Ahmed, “Reputation-based blockchain for secure NDN caching in vehicular networks,” in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Oct. 2018, pp. 1–6.

[102] D. B. Rawat, R. Doku, A. Adebayo, C. Bajracharya, and C. Kamhoua, “Blockchain enabled named data networking for secure vehicle-to-everything communications,” *IEEE Netw.*, vol. 34, no. 5, pp. 185–189, Sep. 2020, doi: 10.1109/MNET.001.1900593.

[103] K. Fan, Q. Pan, K. Zhang, Y. Bai, S. Sun, H. Li, and Y. Yang, “A secure and verifiable data sharing scheme based on blockchain in vehicular social networks,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5826–5835, Jun. 2020, doi: 10.1109/TVT.2020.2968094.

[104] H. Khelifi, S. Luo, B. Nour, H. Moungla, and S. H. Ahmed, “Reputation-based blockchain for secure NDN caching in vehicular networks,” in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Oct. 2018, pp. 1–6, doi: 10.1109/CSCN.2018.8581849.

[105] K. Lei, J. Fang, Q. Zhang, J. Lou, M. Du, J. Huang, J. Wang, and K. Xu, “Blockchain-based cache poisoning security protection and privacy-aware access control in NDN vehicular edge computing networks,” *J. Grid Comput.*, vol. 18, no. 4, pp. 593–613, Dec. 2020, doi: 10.1007/s10723-020-09531-1.

[106] S. Wang, W. Wu, and Z. Zhi, “Varied priority-based data forwarding via NDN in VANET,” in *Proc. IEEE SmartWorld*, Aug. 2019, pp. 574–581, doi: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00137.

[107] M. Al-qutwani and X. Wang, “Smart traffic lights over vehicular named data networking,” *Information*, vol. 10, no. 3, p. 83, Feb. 2019, doi: 10.3390/info10030083.

[108] (2018). *2017 6th International Conference on Communications and Networking, ComNet 2017—Proceedings*. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85050820226&partnerID=40&md5=7afdad229067d09439d0d4718a32653c

[109] A. Tariq, R. A. Rehman, and B.-S. Kim, “Forwarding strategies in NDN-based wireless networks: A survey,” *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 68–95, 1st Quart., 2020, doi: 10.1109/COMST.2019.2935795.

[110] O. Gama, A. Santos, A. Costa, M. J. Nicolau, B. Dias, J. Macedo, B. Ribeiro, F. Goncalves, and J. Simoes, “Evaluation of push and pull communication models on a VANET with virtual traffic lights,” *Information*, vol. 11, no. 11, pp. 1–20, 2020, doi: 10.3390/info11110510.

[111] W. U. I. Zafar, M. A. U. Rehman, F. Jabeen, B.-S. Kim, and Z. Rehman, “Context-aware naming and forwarding in NDN-based VANETs,” *Sensors*, vol. 21, no. 14, p. 4629, Jul. 2021, doi: 10.3390/s21144629.

[112] J. McCarthy, S. R. Chaudhry, P. Kuppuudaiyar, R. Loomba, and S. Clarke, “QoSA-ICN: An information-centric approach to QoS in vehicular environments,” *Veh. Commun.*, vol. 30, Aug. 2021, Art. no. 100351, doi: 10.1016/j.vehcom.2021.100351.

[113] M. Zhang, J. Luo, L. Zhang, X. Yu, T. Xu, and K. Lei, “Comparative analysis of probabilistic forwarding strategies in ICN for edge computing,” *Peer-Peer Netw. Appl.*, vol. 14, no. 6, pp. 4014–4030, Nov. 2021, doi: 10.1007/s12083-021-01219-x.

[114] P. Liu, “Edge computing based ice-snow data analysis with NDN paradigm support,” *Internet Technol. Lett.*, vol. 4, no. 5, p. e271, Sep. 2021, doi: 10.1002/itl2.271.

[115] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Integration of blockchain and cloud of things: Architecture, applications and challenges,” *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2521–2549, 4th Quart., 2020, doi: 10.1109/COMST.2020.3020092.

[116] A. Buzachis, A. Celesti, A. Galletta, M. Fazio, G. Fortino, and M. Villari, "A multi-agent autonomous intersection management (MA-AIM) system for smart cities leveraging edge-of-things and blockchain," *Inf. Sci.*, vol. 522, pp. 148–163, Jun. 2020, doi: 10.1016/j.ins.2020.02.059.

[117] X. Wang and S. Cai, "An efficient named-data-networking-based IoT cloud framework," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3453–3461, Apr. 2020, doi: 10.1109/JIOT.2020.2971009.

[118] J. Lou, Q. Zhang, Z. Qi, and K. Lei, "A blockchain-based key management scheme for named data networking," in *Proc. 1st IEEE Int. Conf. Hot Inf.-Centric Netw. (HotICN)*, Aug. 2018, pp. 141–146, doi: 10.1109/HOTICN.2018.8605993.

[119] O. Attia, I. Khoufi, A. Laouiti, and C. Adjih, "An IoT-blockchain architecture based on hyperledger framework for healthcare monitoring application," in *Proc. 10th IFIP Int. Conf. New Technol., Mobility Secur.*, 2019, pp. 1–5, doi: 10.1109/NTMS.2019.8763849.

[120] H.-K. Yang, H.-J. Cha, and Y.-J. Song, "Secure identifier management based on blockchain technology in NDN environment," *IEEE Access*, vol. 7, pp. 6262–6268, 2019, doi: 10.1109/ACCESS.2018.2885037.

[121] K. Asaf, R. A. Rehman, and B.-S. Kim, "Blockchain technology in named data networks: A detailed survey," *J. Netw. Comput. Appl.*, vol. 171, Dec. 2020, Art. no. 102840, doi: 10.1016/j.jnca.2020.102840.

[122] Z. Yu, A. Dong, X. Wei, S. Guo, and Y. Yan, "Hybrid chain based hierarchical name resolution service in named data network," in *Advances in Intelligent Systems and Computing*, C.-N. Yang, S.-L. Peng, and L. C. Jain, Eds. Cham, Switzerland: Springer, 2020, pp. 629–637.

[123] K. Lei, S. Huang, J. Huang, H. Liu, and J. Liu, "Intelligent eco networking (IEN) II: A knowledge-driven future internet infrastructure for value-oriented ecosystem," in *Proc. 2nd Int. Conf. Hot Inf.-Centric Netw. (HotICN)*, Dec. 2019, pp. 31–36, doi: 10.1109/HotICN48464.2019.9063217.

[124] F. K. Flores and M. Peradilla, "A framework for named networking on edge AI," in *Proc. 13th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2022, pp. 399–404, doi: 10.1109/ICUFN55119.2022.9829714.

[125] C. Campolo, G. Lia, M. Amadeo, G. Ruggeri, A. Iera, and A. Molinaro, "Towards named AI networking: Unveiling the potential of NDN for edge AI," in *Proc. Int. Conf. Ad-Hoc Netw. Wireless*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 12338, 2020, pp. 16–22.

[126] A. Abane, P. Muhlethaler, M. Daoui, and H. Afifi, "A down-to-earth integration of named data networking in the real-world IoT," in *Proc. 6th Int. Conf. Future Internet Things Cloud Workshops (FiCloudW)*, Aug. 2018, pp. 243–249, doi: 10.1109/W-FiCloud.2018.00046.

[127] M. Babar, M. S. Khan, F. Ali, M. Imran, and M. Shoaib, "Cloudlet computing: Recent advances, taxonomy, and challenges," *IEEE Access*, vol. 9, pp. 29609–29622, 2021, doi: 10.1109/ACCESS.2021.3059072.

[128] O. H. Ahmed, J. Lu, A. M. Ahmed, A. M. Rahmani, M. Hosseinzadeh, and M. Masdari, "Scheduling of scientific workflows in multi-fog environments using Markov models and a hybrid salp swarm algorithm," *IEEE Access*, vol. 8, pp. 189404–189422, 2020, doi: 10.1109/ACCESS.2020.3031472.

WAN MUHAMMAD HAZWAN AZAMUDDIN received the M.Sc. degree in computer science from the Technical University of Malaysia (UTeM), in 2016. He is currently pursuing the Ph.D. degree with the Faculty of Information Science and Technology (FTSM), Universiti Kebangsaan Malaysia (UKM), Malaysia. He has published several articles in peer-reviewed international journals. His current research interests include networking, future internet technology, and mobility NDN.

AZANA HAFIZAH MOHD AMAN received the B.Eng., M.Sc., and Ph.D. degrees in computer and information engineering from International Islamic University Malaysia. She is currently a Senior Lecturer with the Research Center for Cyber Security, Faculty of Information Science and Technology (FTSM), Universiti Kebangsaan Malaysia (UKM), Malaysia. Her research interests include computer system and networking, information and network security, the IoT, cloud computing, and big data.

HASIMI SALLEHUDDIN is currently a Senior Lecturer with the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia. His research interests include computer security and networks, and management information systems.

KHALID ABUALSAUD (Senior Member, IEEE) is currently with the Department of Computer Science and Engineering, Qatar University, Qatar. He has more than 25 years of professional experience in information technology. He teaches courses in hardware and software systems. He is active in getting research funding from different sources, including the Qatar National Research Foundation, the Supreme Committee for Delivery and Legacy (FIFA 2022), and some other organizations in Qatar. He is also a LPI of the NPRP 10-1205-160012 Research Project, which achieved significant outcomes. He has participated actively in organizing several IEEE international conferences in Qatar, namely ICIoT 2020, IEEE WCNC 2016, PLM 2015, AICCSA 2014, RelMiCS 2011, and AICCSA 2008. His research work has been presented at international conferences and journals. His research interests include health systems, wireless sensors for IoT applications, cybersecurity, cloud computing, and computer network protocols. He has served as a technical program committee (TPC) member and the chair for various reputable IEEE conferences. He received several awards from different local and international organizations. He served as the Guest Editor for Connected Healthcare Special Issue for *IEEE Network*. He is an Associate Editor of *IET Quantum Communication*.

NORHISHAM MANSOR received the M.Sc. degree in computer science from the Technical University of Malaysia (UTeM), in 2014. He is currently a Vocational Training Officer with the Advance Technology Training Center (ADTEC) Batu Pahat. He has published several articles in peer-reviewed international journals. His current research interests include networking security, future internet technology, and NDN security.