IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 18 October 2022, accepted 10 November 2022, date of publication 21 November 2022,
date of current version 28 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3223667

SURVEY

Application Areas of Information-Centric Networking: State-of-the-Art and Challenges

LALITHA CHINMAYEE M. HURALI AND ANNAPURNA P. PATIL, (Senior Member, IEEE)
Department of Computer Science and Engineering, Ramaiah Institute of Technology, Bengaluru, Karnataka 560054, India

Corresponding author: Lalitha Chinmayee M. Hurali (lalithachinmayee@gmail.com)

ABSTRACT The Information-Centric Network (ICN) paradigm has gained popularity since its inception. The host-based IP networks were not primarily designed to handle scenarios that it is exposed to on the current Internet. In that direction lot of research has been happening to develop applications such as web applications, multimedia streaming, the Internet of Things, Wireless Sensor Networks and Vehicular networks. In addition, new ICN application areas, such as social networks, Industrial IoTs, etc., are emerging. This review investigates the possible application areas and their deficiencies evenly, broadly and at a certain level of depth with focus on security, scalability, IP interoperability, modularity and other application specific aspects. We discuss the current state-of-the-art in these ICN-based applications and the existing limitations. A comparative analysis of the literary works available is performed to understand the research gaps available, and a detailed discussion of the challenges in each area is provided. We conclude the review with future challenges in the application development with the ICN paradigm to reap its architectural benefits.

INDEX TERMS Content-centric networks, information-centric networks, named data networking, network security.

I. INTRODUCTION

Due to the advent of data-intensive applications, the current Internet Protocol (IP) based internet faces many challenges in its host-centric infrastructure. A paradigm shift from a host-centric approach to an information-centric approach is beneficial in data-intensive applications optimized solely for content retrieval on the Internet. The information-centric approach focuses on disseminating information objects rather than the conversation between the hosts. This approach has paved the way for a new redesigned Internet architecture called the Information-Centric Networks (ICNs) [1].

The ICN communication concentrates on what to communicate instead of whom to communicate with, as in the IP-based networks. ICN delivers the information independent of its location, often termed an information-centric abstraction. In ICNs, content names are used for communication rather than the host addresses. The named content is cached in the network using routers capable of storage termed content routers. This feature of ICNs is called in-network caching and is one of the unique features of the ICN. Security of the content is an intrinsic feature in ICN architecture as the named contents are secured. The content names are self-certified by their producer through encryption [2], [3].

The research community has proposed many representative ICN architectures like Content-Centric Networking (CCN) [4], Named Data Networking (NDN) [5], [6], MobilityFirst (MF) [7], eXpressive Internet Architecture (XIA) [8], Data-Oriented Network Architecture (DONA) [9], Network of Information (NetInf) [10], PSIRP/PURSUIT [11]. We discuss each of the above ICN architectures in brief in the following section along with the key functionalities of the ICN architecture.

A. KEY FUNCTIONALITIES OF ICN PARADIGM

This subsection briefly discusses the key functionalities of the ICN paradigm, such as naming, routing and forwarding, in-network caching, and intrinsic security, to name a few.

1) NAMING

The basic crux of the ICN paradigm is that information can be named and addressed independently of its location. This very

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

concept of location-independent information retrieval makes the communication receiver or client driven. The ICN names the content objects in the network as Named Data Objects (NDOs), consisting of a name, the content and metadata. The design of an NDO is particular to an ICN architecture; however, the naming scheme can be either flat or hierarchical. The flat naming scheme is self-certifying using hash techniques, thus ensuring name-data integrity. However, this scheme is not human-readable and scalable. On the contrary, the hierarchical scheme has a structure with prefixes and is human-readable and scalable. The choice of ICN naming scheme is a tradeoff against the routing and usability of ICN-based applications [1].

2) ROUTING AND FORWARDING

In general, there are two different routing and forwarding approaches in ICN-based Internet applications, namely: Name resolution and Name based Routing. Name resolution is a two-step approach (mapping and forwarding) where an ICN client searches for content by NDO's name. Usually, an entity called the Name Resolution Service (NRS) performs the name-to-content translation and forwards the request to the content producer. This approach is a guaranteed way of accessing the content. However, NRS could require significant storage and pose as a single point of failure in the network. The latter Name based Routing approach is a one-step approach where the content routers forward the NDO request hop by hop by its name. This approach is not a guaranteed way of routing and forwarding as the process is done hop by hop through the content routers [1].

3) IN NETWORK CACHING

The interesting feature of the ICN paradigm is the ability of the network entities to cache the content to make the NDOs easily accessible. The NDOs are cached locally on the network nodes, networks or content routers. This offloads the traffic away from the content producer and improves the response time of the NDO requests. Multicasting and retransmission become easy with in-network caching, and cache placement and replacement policies are the core of incorporating in-network caching in ICN-based applications.

4) INTRINSIC SECURITY

The ICN paradigm provides name-data integrity and data origin authentication implicitly. The ICN caching and naming exposes the system to Denial of Service attacks, cache pollution attacks and snooping attacks etc. The ICN architecture involves digital signature-based methods to provide content integrity. Another essential aspect of ICN intrinsic security is providing content and user authenticity. Security is achieved through trust management mechanisms through hash tables. Data and user privacy is addressed in ICN through cryptographic filters. In addressing all the above areas, such as integrity, authenticity and privacy, the scalability and storage issues come to the forefront of the ICN application development [87].

One of the pioneer reviews in application and service provision over ICN architecture is discussed in [12]. Although the work is the first of its kind, it lacks a detailed discussion and analysis of research works in each application area of ICN. Our work sheds light on each of the application areas with a focus on new applications of ICN such as Social Networks, Anamoly Detection, and Industrial IoTs. It comprehensively discusses the application requirements, the recent literature review and their comparison and identifies the existing research gap.

The main contribution of this review work is as listed below

- A comprehensive discussion on the rise of the ICN paradigm and a brief on the available future internet architectures.
- A compilation of the possible security threats to ICN architecture and the application and services is provided.
- A detailed discussion on the prerequisites for ICN application areas and the current state-of-the-art literary works is provided. A comparative analysis of the state-of-the-art literature is also provided.
- Finally, we discuss the open research areas in each application area to enable future research works in that direction.

The organization of the review is as follows: Section I provides an introduction to the ICN paradigm and its benefits over traditional IP-based networks. A brief introduction to the future internet architecture is provided in Section II. Section III compiles the possible security threats to ICN architecture, its application and services. A detailed analysis of each ICN application area and the research challenges are provided in section IV. Finally, section V concludes the review.

II. ICN ARCHITECTURES

A. CONTENT-CENTRIC NETWORKING (CCN) / NAMED DATA NETWORKING (NDN)

NDN is a branch of the CCN project, and both have the same characteristics, such as hierarchical naming, in-network caching, and named routing and forwarding. There are two packet types in the CCN/NDN network, the Interest packet and the Data packet. The client in the network requests content using an interest packet to the network using its content name. The content is sent back to the client through a data packet either by a Content Store (CS) or the content producer. A router in CCN/NDN network has three data types: Content Store (CS), Pending Interest Table (PIT), and, Forwarding Information Base (FIB). Upon receiving an interest packet, a router looks into its CS for the content name. If it is not available in the CS, it checks the PIT for an entry related to the current interest packet. If PIT has an entry, the router drops the interest packet or creates a new PIT entry and forwards the interest packet using the FIB. The data packet traverses the interest packet path in the reverse direction. Any router in the data packet's path forwards the content to the interfaces according to the PIT entries and may also cache the content in its CS [4], [5], [6].

B. PUBLISH-SUBSCRIBE INTERNET ROUTING PARADIGM (PSIRP)/ PUBLISH-SUBSCRIBE INTERNET TECHNOLOGY (PURSUIT)

PSIRP/PURSUIT is based on publish/subscribe protocol. A PSIRP/PURSUIT network comprises three network entities: Rendezvous Nodes (RNs), a topology manager and forwarders. A content producer publishes their content using a PUBLISH message to its nearest RN (local RN). The local RN routes the PUBLISH message to its designated RN (which stores the content names) using a Distributed Hash Table (DHT). Any client interested in data sends a SUBSCRIBE message to its local RN, which will be routed to the designated RN using DHT. On receiving a SUBSCRIBE message, a designated RN asks the topology manager to generate a path between the content producer and the client through the forwarders [11].

C. MOBILITYFIRST (MF)

MobilityFirst ICN architecture focuses on a user's mobility. An MF network consists of 3 network entities: devices, information objects and services. Each of these entities is assigned a globally unique identifier (GUID) that can be translated into a network address. A content producer requests a GUID from the naming service and registers the same with the global name resolution service (GNRS). This GUID is mapped to a set of connected GNRS servers. A client sends a GET message containing the GUID of required content (obtained from the Name Certification Service (NCS)) and its GUID to a nearby router. The local router receives the network address corresponding to the requested GUID with the help of GNRS. The forwarding routers in the network add the destination address to the GET message and send it into the network, and updates the destination address in the GET message as it is forwarded in the network. The content producer sends the content to the client/ forwarding router GUI back to the client, in the same way, discussed previously [7].

D. eXpressive INTERNET ARCHITECTURE (XIA)

eXpressive Internet Architecture (XIA) proposes an ICN-based clean slate architecture supporting content, services and users. XIA aims to incorporate evolvability and security into the Internet architecture. eXpressive Internet Protocol (XIP) is the core of XIA. XIA supports entities such as hosts, content and services (termed principals) while also providing support for future unknown principals. XIA also provides intrinsic security and the flexibility mentioned above in communication [8].

E. DATA-ORIENTED NETWORK ARCHITECTURE (DONA)

The DONA network involves flat naming and hierarchical naming resolution. Routing in DONA involves FIND and REGISTER processes. A content producer sends a REGISTER message to the Resolution Handle (RH), adding it to its three-tuple information base hash of content producer's public key: content label, next hop, distance. Successively each RH forwards this tuple information to its parent RH till the root RH. When a client requires content, it sends a FIND message to its local RH using the corresponding content name. The FIND message is propagated to the parent RH in the hierarchy till a match is found. Once an appropriate RH is found, the content request is forwarded to the content producer using the three-tuple information base, either using the underlying IP network or using the path symmetry (breadcrumbs approach) [9].

F. NETWORK OF INFORMATION (NetInf)

A NetInf network consists of routers with storage and a Name Resolution Service (NRS). Content retrieval in NetInf happens in two steps: name resolution / name-based routing. A content producer registers its content with NRS in the name resolution step. A client can request content, and routing forwarders will deliver it through the available cache. On the other hand, in name-based routing, a client sends a GET message using the name of the content into the network. This message is forwarded to the router using name-based routing, and the content is sent back to the client on its availability [10].

Table 1 compares the various representative ICN architectures on different aspects such as design goals, network attributes (naming, caching, routing), packet/ message types, network entities and security mechanisms employed in each architecture.

III. SECURITY AND PRIVACY IN ICN

Security and privacy in ICN are inherently incorporated into the ICN network architecture. The intrinsic security mechanisms in different ICN architectures are listed briefly in Table 1.

The ICN paradigm stresses security and privacy by design. Most ICN representative architectures were initially developed to provide the following security and privacy features by design: trust, data origin authentication, peer entity authentication, data integrity, authorization and access control, accountability, availability, data confidentiality, traffic flow confidentiality and anonymous communication. While digital signatures and certificates address trust, data origin authentication, integrity and accountability, Cryptographic hash techniques provide integrity to the ICN communication. Lastly, path consent mechanisms and Access Control Lists secure features such as authorization and access control and accountability. The availability aspect is not addressed holistically in ICN.

Moreover, weak countermeasures such as path consent verification and Interest Key Binding (IKB) rules are proposed for the same. Privacy aspects such as data confidentiality are protected by payload and end-to-end encryption, and anonymity is provided by applications such as Tor and Andana. Features such as peer entity authentication and traffic flow confidentiality are unaddressed by any ICN architectures. The above discussion briefly summarizes the security and privacy requirements of an ICN application and discusses

TABLE 1. Comparison of various ICN architectures.

Characteristics	CCN/NDN	PSIRP/PURSUIT	MobilityFirst	XIA	DONA	NetInf
Design goal	Large-scale content distribution	A suite of ICN protocols	User mobility	Evolvability and Intrinsic security	Data retrieval and service access	Scalability
Naming Scheme	Hierarchical	Flat	Flat	Flat	Flat	Flat
In Network Caching	✓	✓	✓	✓	✓	✓
Named routing and forwarding	✓	✓	✓	✓	✓	✓
Intrinsic Security	✓	✓	✓	✓	✓	✓
Routing	Name-based routing using FIB and PIT	Name-based routing using Topology Managers and Forwarders Name Resolution using RN	Generalized Storage Aware Routing (GSTAR)	eXpressive Internet Protocol (XIP)	Name resolution using a route-by-name paradigm	Name-based routing and Name Resolution using NRS
Packet/Message types	Interest Packets Data Packets	Publish message Subscribe message	GET message	XIA packets	FIND and REGISTER packets	GET message
Network Entities	Client Content Producer	Rendezvous Nodes Topology Manager Forwarders Content Producers Clients	Devices (Routers) Information Objects Services (GNRS servers, NCS)	Clients/Hosts Content Services (Principals)	Content Producer Resolution Handler	Routers NRS
Security Mechanisms	Self-certifying signature	Elliptic curve cryptography / zFilters / zFormations	Self-certifying signature (GUIDs)	Cryptographically secured identifiers	Self-certifying signature	Named Information URL scheme

the available mechanisms. Thus the security and privacy by the design concept of the ICN paradigm are not fully accomplished. There is a vital requirement for a comprehensive set of security and privacy features among the ICN architectures to attain security and privacy by design paradigm. [96]

Although ICN security feature mitigates some of the legacy attacks relevant in host-centric architecture, it also opens a door for new security attacks with its new security model. Like any other computer network, Confidentiality, Integrity and Availability (CIA triad) is the vital objectives in developing a security model for a network. A threat to a network security model affects either one or many out of the CIA triad objectives. In addition, a threat in an ICN network can affect naming, routing, and/or caching.

A. COMMON THREATS IN ICN

In this section, we discuss the common threats in an ICN network and segregate them as per the CIA triad for clarity in understanding (Table 2) [14], [15]. We also provide the security objective and the network aspect (such as naming, routing and caching) that each threat affects the ICN network as per the CIA triad and [3]. In classifying the CIA triad information, we consider data confidentiality and privacy under Confidentiality and data integrity and system integrity under Integrity [16]. We refer the reader to look into the surveys [14], [15] for a detailed understanding of the threats mentioned in Table 2.

The research on the security and privacy aspect of ICN architectures is not addressed in detail as compared to the research on the threats available and their countermeasures in host-centric networks. In this section, we briefly discuss various possible threats and their mitigation approaches used in general and not specific to ICN architectures. We categorize the threats based on the attacker's target in the ICN architecture as naming, routing, caching and other miscellaneous targets.

TABLE 2. Common threats in an ICN network.

Threats		Security Objectives			Attackers target in ICN
		C	I	A	
Watchlist		✓	✓	✓	Naming
Sniffing		✓	✓	✓	Naming
Scanning		✓	×	×	Naming
Protocol Attack	Prefix matching Attack	✓	×	×	Naming
	Scoping Attack	✓	×	×	Naming
DDoS	Infrastructure exhaustion	×	×	✓	Routing
	Source Exhaustion	×	×	✓	Routing
	Mobile Blockade	×	×	✓	Routing
	Interest Flooding	×	×	✓	Routing
	Timing	×	×	✓	Routing
Spoofing	Jamming	×	×	✓	Routing
	Hijacking	×	×	✓	Routing
	Interception	✓	×	✓	Routing
Man in the Middle Attack		✓	×	×	Routing
Time Analysis		✓	×	×	Caching
Bogus Announcements		✓	×	✓	Caching
Cache Pollution	Random request/ False Locality	✓	×	✓	Caching
	Unpopular request/Locality disruption	✓	×	✓	Caching
Cache Spoofing	Cache monitoring	✓	×	×	Caching
	Object discovery	✓	×	×	Caching
	Flow Cloning	✓	×	×	Caching
Packet mistreatment		✓	✓	×	Miscellaneous
Breaching the signer's key		✓	✓	×	Miscellaneous
Unauthorized access		✓	×	✓	Miscellaneous

B. ATTACKS ON NAMING AND THE POSSIBLE COUNTERMEASURES

Watchlist, sniffing, scanning and protocol attacks (scoping and prefix matching) are some attacks on naming in ICN architectures. In case of a watchlist attack, an attacker maintains a predefined list of named contents to filter or delete such content. A sniffing attack is similar to a watchlist, but the only difference is sniffing attack happens by dynamically analyzing the requests or the contents on the network. In a port scanning attack, an attacker sends many content requests to all the available ports to learn the port details and status for further attacks. The adversaries learn the scope of the ICN packets to gain access to sensitive information in case of a scoping attack. In the case of prefix-matching attacks, the adversaries misuse the prefix in the ICN messages to understand the content a client consumes. The attacks on naming can be prevented by countermeasures such as the usage of firewalls and intrusion prevention systems.

C. ATTACKS ON ROUTING AND THE POSSIBLE COUNTERMEASURES

DDoS, spoofing, and Man in the Middle attacks are common attacks under routing in ICN. DDoS attacks involve infrastructure exhaustion, source exhaustion, mobile blockade, interest flooding, and timing attacks. In infrastructure and source exhaustion attacks, an attacker sends content requests for available or unavailable content repeatedly to either make the service deniable through the whole of the network or one particular source. On the other hand, a mobile attacker blocks the available network by continually sending requests to all the available networks in the surroundings. In interest flooding attacks, legitimate users are denied the service due to an unreasonably large number of interest requests from an attacker. Similarly, in a timing attack, an attacker succeeds in service denial by making the access time large enough for legitimate users.

All in all, DoS and DDoS have been widely studied attacks in ICN literature, and countermeasures involve packet inspection, encryption and signature-based methods. Spoofing attacks, namely jamming, hijacking, and an interception, are another class of attacks on routing in ICN. Jamming interrupts the information flow in the ICN network by sending malicious content requests. In the case of hijacking, the attacker shares the malicious routes to hijack the network on a large scale. Lastly, in interception attacks, the attacker records the valid routes in the network to intercept the communication between legitimate uses of the network. The three mentioned spoofing attacks could be mitigated with countermeasures such as filtering and using cryptographic techniques in the literature. Another major routing-based attack is the man-in-the-middle attack, where an attacker hears and alters the content communicated between legitimate users. Such attacks can be detected with countermeasures such as firewalls and intrusion prevention systems.

D. ATTACKS ON CACHING AND THE POSSIBLE COUNTERMEASURES

The most common caching-related attacks in ICN are time analysis, bogus announcements, cache pollution/poisoning and cache spoofing. The time analysis attack involves an adversary measuring the time difference between cached and uncached contents to invade a user's privacy. Cache-based timing attacks can be defended using techniques such as time skewing, flushing, warming or minimizing the timing accuracy available to the attacker [97]. The bogus announcement attacks involve an attacker sending out content requests at a frequency far more quickly than the network can handle. Hence, some of the unattended requests lead to erroneous or incomplete requests affecting the proper functioning of caching. In the case of cache pollution/poisoning attacks, an attacker aims to either disrupt the cache locality or to make it false. Cache poisoning attacks have been widely studied in ICN literature. The famous defense mechanism is signature-based methods, cache verification methods and the recent machine learning-based methods.

E. MISCELLANEOUS ATTACKS AND THE POSSIBLE COUNTERMEASURES

Miscellaneous attacks on the ICN networks are packet mistreatment, breaching the signer's key and unauthorized access. Packet mistreatment involves an attacker modifying the packet contents or sending multiple copies of the same, as in a replay attack. Some of the countermeasures available in the literature are filtering and signature-based methods. The distributed nature of the named content in ICN makes it vulnerable to unauthorized access. Common countermeasures involve path control mechanisms and access control lists.

IV. INFORMATION-CENTRIC NETWORK-BASED SOLUTIONS IN VARIOUS APPLICATION AREAS

A. WEB APPLICATION

Many researchers have studied the integration of web applications over the ICN architecture to arrive at future Internet. One of the pioneer efforts in this direction is discussed in [17]. The authors have studied the similarities between NDN's push-pull architecture and the Hypertext Transfer Protocol (HTTP) web application's request-reply architecture. In addition, they discuss and analyze the possible communication patterns to run RESTful web services (Representational State Transfer) over the NDN architecture. A bird's eye view of the possible threats in each communication pattern such as DoS, DDoS flooding, amplification and reflection attack is also provided. The authors conclude that the current NDN architecture needs to be worked upon to accommodate the RESTful web services. In [18], the authors propose a native CCN-based web browser, CCNBrowser and a CCN-based web server, CCNxTomcat, to provide native support to CCN web applications. The work also supports interoperability with the HTTP protocol and improves throughput compared to the traditional IP-based web applications.

Studies in [19] have shown the feasibility of dynamic web applications over NDN architecture through a session-based approach. This approach mitigates the packet retransmission problem by introducing a session ID to establish a session for dynamic web content retrieval in NDN. The framework has shown good performance improvement in network utilization and service delay. However, incorporating a session ID can result in a privacy breach as the network users can be tracked if the ID is compromised. The paper does not discuss any mitigation approach for the possible security threats to the architecture.

HTTP over a hybrid ICN (hICN) architecture is presented in [20]. The researchers map the HTTP semantics to ICN names to benefit from the inherent features of ICN architecture. HTTP semantics are achieved on the hICN architecture using reverse pull-based communication. The HTTP over hICN is prone to reflection attacks, and the authors propose a client signature-based mitigation approach to tackle the threat. In the paper [21], the authors discuss a content-oriented interoperable COIN network for current and future internet architectures. They mainly focus on static and content retrieval in IP, NDN and MobilityFirst architectures through Object Resolution Services. They use encryption (MD5, SHA-1 and SHA-256) and iterative signature-based schemes (RSA, ECDSA, EdDSA) to ensure security. The authors discuss the possible threats in COIN architecture, such as DoS and DDoS attacks (bandwidth depletion, reflection attack, interest flooding, cache poisoning) and their mitigation approaches.

Modern web applications must ensure scalability, security and user expectations. A web application must be modular, decentralized and optimized to handle current complex scenarios (cloud hosting, cross-platform etc.) [22]. A consolidated overview of the current literature in this area is provided in Table 3. And we discuss the future research directions required in web application development over the ICN architecture as below:

- Security: Modern web application requires built-in security instead of an add-on feature. Although ICN provides inherent security to its applications, there is a lack of research investigating legacy web application threats such as injection, access control, data exposure etc. However, there is a good start in this direction as most of the literature we reviewed studies threats such as reflection attacks and DoS attacks.
- Scalability: Since the Internet currently is beaming with billions of users, the scalability of web applications will remain an area of investigation till the end of time. Only two of the recent research [20], [21] address the scalability feature. We suggest that all future research works in this area address the scalability feature as it is a crucial aspect in real-world deployment scenarios.
- Interoperability with IP networks and native support in ICN: As the ICN paradigm is little more than a decade old, migration from IP is a complex activity. Therefore, any ICN-based web applications research needs to maintain interoperability and yet provide the application as a native feature instead of as an overlay.
- Modularity: A modern web application over ICN must support a modular microservices-based scheme to utilize the advantages it adds, such as reduced security surface area, easy maintenance etc. Modern web tools such as RESTful APIs and GraphQL should be studied in-depth to analyze the pros and cons over ICN architecture.

As of the current research progress, there is no one size fits all solution for web applications over ICN architecture. The researchers need to decide whether the open challenges discussed above should be considered as architectural modifications in ICN or as a part of application development.

B. MULTIMEDIA STREAMING

Multimedia streaming is one of the key application areas of ICN due to its data-centric abstraction, in-network caching and multicast behavior. One of the first works on multimedia streaming over an ICN network is discussed in [23]. The authors propose an android TV-based HTTP live video streaming (HLS) application over NetInf architecture. The implementation demonstrates the feasibility and performance of HLS over NetInf for efficient multicasting of video. In the paper [24], the authors propose a MPEG Dynamic Adaptive Streaming over HTTP (DASH) multimedia streaming approach over CCNx implementation. Their evaluation shows that their work matches the existing IP-based streaming solutions in performance but does not outperform them. There are still many challenges to be addressed as this work was proposed at the very early onset of CCN for multimedia streaming. A Scalable Video Coding (SVC) based adaptive streaming over ICN architecture is proposed in [25] to reduce data redundancy. The work evaluates a comparison of Advanced Video Coding (AVC) and SVC over ICN for live video streaming. The paper also discusses the challenges in integrating the two technologies, such as bandwidth unpredictability and cache awareness and mitigation approaches. The document [26] by the Internet Research Task Force (IRTF) discusses the consequences of video distribution in future ICN-based architectures for Netflix and P2P-like scenarios. The authors suggest the usage of DASH over CCN for efficient video dissemination and evaluate the scenarios using an open-source testbed and dataset provided in [27]. The research challenges and the concerns regarding Quality of Experience in the video services over ICN are also provided.

An evaluation of pull-based adaptive video streaming over NDN is provided in [28]. The work focuses on the MPEG DASH SVC encoded video streaming using different adaptation techniques such as no adaptation, rate-based and buffer-based adaptation. The results show the advantages of their approach over the existing MPEG DASH over TCP/IP networks. The paper [29] presents network coding enabled DASH video streaming over NDN architecture. They claim that using network coding and multipath features in NDN helps in improved data packet loss handling and throughput and reduced network load in Netflix-like scenarios, in turn reducing overall cost in video dissemination. The authors in [30] discussed the applicability of ICN architecture in multimedia delivery for Vehicular Adhoc Networks (VANETs). The cost is minimized considering a mixed inter programming optimization besides gain in delay, jitter, seamless playback, and QoE compared to the IP-based solutions. Another adaptive DASH video streaming solution is discussed in [31] but with bitrate feedback to avoid network congestion. This approach limits the viewer with a high bitrate with the least QoE degradation with early feedback. The simulation results have shown that their work improves QoE for different bitrate adaptations such as rate-based and hybrid-based.

Authors in [32] discuss a panoramic live video streaming application based on tiles over NDN. The video frames are tiled and edge transcoded to reduce the load on traffic. A dynamic adaptive SVC encoded MPEG DASH video streaming over NDN is proposed in [33]. Implementing the probabilistic caching and buffer and reorder forwarding policies in this work has improved the player bitrate, video stall duration and frequency. In [34], a bitrate aware cache partitioning and placement scheme is discussed to provide

TABLE 3. Comparison of research works in web applications over ICN.

Ref.	Research direction	ICN architecture	Interoperabiity with IP	User scalability	Add on Security	Security threat	Mitigation approaches
[17]	RESTful web services over NDN	NDN	×	×	✓	DoS, DDoS, Amplification, Reflection attack	Stateful forwarding and packet inspection
[18]	A native web browser and server for CCN	CCN	✓	×	×	-	-
[19]	Dynamic web applications over NDN	NDN	×	×	×	Privacy	-
[20]	Hybrid ICN integration with IP	-	✓	✓	✓	Reflection attacks	Client signature
[21]	Content retrieval over the COIN architecture	NDN and MobilityFirst	✓	✓	✓	DoS and DDoS	Encryption and signature-based schemes

good QoE in the DASH video streaming over ICN. The scheme helps stabilize the bandwidth/bitrate fluctuation by choosing content appropriate caching scheme. The proposed method provides better video quality QoE over the existing cache placement policies in NDN. A Multi-access Edge computing-based DASH streaming over NDN is proposed in [35] to improve rate estimation and user QoE. They simulate DASH streaming over ndnSim to achieve a more accurate and stable rate estimation against the state-of-the-art. An NDN multicast-based adaptive video streaming in WLAN is proposed in [36]. They evaluated their scheme with different network topologies over NDN with real-world. The results show improvement in bitrate delay and stall time in video streaming.

In [37], an SVC-aware caching strategy for dynamic MPEG DASH adaptive streaming over NDN is considered. The authors propose two strategies: reverse probabilistic caching and linear probabilistic caching, which are SVC aware. Furthermore, these caching strategies perform better than SVC agnostic caching strategies in improving cache hit ratio, latency and average bitrate. An explicit congestion notification for adaptive video streaming over NDN is discussed in [38] to improve QoS and QoE. The cache efficiency and the video quality is improved due to the explicit congestion information delivered by the router to the client. As seen from Table 4, most of the research works in multimedia streaming over ICN addressed adaptive video streaming, which is the need of the hour due to mobile wireless environments. However, on analyzing from Table 4, a few additional research considerations need to be addressed to attain maturity in this area.

- Security: Most research works completely ignore the possibilities of security attacks in multimedia streaming applications over ICN. The confidentiality and availability of streaming data still remain an important area to be addressed.
- Scalability: Scalability was one of the significant factors that led to drifting from IP-based to ICN-based architecture. Nevertheless, this factor is unaddressed mainly in the research works discussed except in a few [31], [32]. There needs to be more research in this area as the primary streaming applications such as sports streaming, and entertainment concerts are potential candidates for large-scale ICN deployment.
- Digital Rights Management (DRM): Although a subclass of security aspects, DRM requires specific attention in multimedia streaming. We urge the researchers to inspect this area to leverage multimedia streaming over ICN as a whole entity.
- Interoperability with IP networks: As discussed previously under the web application section, an understanding of IP interoperability is required rather than just implementation on clean slate ICN architecture for seamless transition from IP.

The majority of the works focus solely on the quality of experience for the user. Researchers need to note that the gaps discussed above can also improve the QoE over and above the existing values. In addition, the researchers can investigate the areas of virtual reality, cross-platform and cloud-based deployment (Android, windows), to name a few.

C. WIRELESS SENSOR NETWORKS (WSNs)/INTERNET OF THINGS (IoT)

Researchers have identified that the information-centric nature of ICNs is beneficial to the field of WSNs and, in turn, IoT due to the mobile and dynamic nature of its components. Also, the primary request/response way of communication in ICNs helps to build an IoT/WSN in an easy and fast way as compared to IP-based networks. The literature in the field of information-centric IoTs (IC-IoTs) and information-centric WSNs (IC-WSNs) is very rich, and prior to our work, there were many detailed reviews in this field. We take the opportunity to highlight the existing review to eliminate any redundancy for the readers published in recent times [39], [40], [41], [42], [43]. Henceforth we discuss the progress in IC-IoTs/ IC-WSNs research as a continuation of the prior published review articles. We take forward this section in two significant parts: IC-WSNs and IC-IoTs, to briefly shed light on the existing approaches.

1) INFORMATION-CENTRIC WIRELESS SENSOR NETWORKS (IC-WSNs)

The authors in [44] discuss an Information-centric protocol for WSNs to gather big data. The ICN approach in data gathering helps to reduce overhead in the WSNs, leading to improved scalability. The protocol is fine-tuned for dynamic

TABLE 4. Comparision of research works in multimedia streaming over ICN.

Ref.	Research direction	ICN architecture	Interoperabiity with IP	User scalability	Add on Security	Security threat	Mitigation approaches
[23]	HLS video streaming over NetInf	NetInf	×	×	×	-	-
[24]	MPEG DASH multimedia streaming over CCNx	CCNx	×	×	×	-	-
[25]	SVC encoded live video streaming over ICN	NDN	×	×	×	-	-
[26]	Adaptive DASH video streaming over CCN	CCN	×	×	×	-	-
[28]	Adaptive DASH video streaming over NDN	NDN	×	×	×	-	-
[29]	Adaptive DASH video communication streaming with network coding over NDN	NDN	×	×	×	-	-
[30]	Cost-effective multimedia delivery over NDN in VANETs	NDN	×	×	×	-	-
[31]	Adaptive DASH streaming video with bitrate feedback	NDN	×	✓	×	-	-
[32]	Panoramic tile-based live video streaming application	NDN	✓	✓	✓	Integrity and authentication	Hash-based Message Authentication Code (HMAC)
[33]	SVC encoded Adaptive MPEG DASH over NDN	NDN	×	×	×	-	-
[34]	Bitrate aware cache partitioning in adaptive video streaming over ICN	NDN	×	×	×	-	-
[35]	Multi-access Edge computing-based DASH streaming over NDN	NDN	×	×	×	-	-
[36]	NDN multicast-based adaptive video streaming in WLAN	NDN	×	×	×	-	-
[37]	SVC aware probabilistic caching in adaptive video streaming over NDN	NDN	×	×	×	-	-
[38]	Explicit cache notification for adaptive video streaming over NDN	NDN	×	×	×	-	-

WSNs where sensor nodes are mobile to reduce/eliminate data loss. In the paper [45], an architectural extension to NDN to presented to accommodate cluster-based WSNs. The extended architecture includes an energy-efficient naming and forwarding scheme and is evaluated in a surveillance and monitoring use case. The results show an improvement in the considered performance metrics and ensure seamless mobility in IC-WSNs over NDN.

A caching strategy based on the WSN node's placement in an IC-WSN is discussed in [46]. The caching strategy involves cache placement and replacement policies to enable energy-efficient IC-WSNs in a smart university campus scenario. The results show that the distance and degree aware cache placement and popularity-based cache replacement policies improve energy efficiency, cache hit and replacement rate in IC-WSNs. In [47], a user authentication scheme using wireless earphones in IC-WSNs is presented. The solution in the rhythm-based tapping method involves deep learning and machine learning methods for brute attack and video and imitation attack detection.

a: UNDERWATER WSNs

Synergetic DoS (SDoS) attack in underwater WSNs based on the ICN paradigm is discussed [48]. The DoS attack involves interest flooding causing a security threat to all the data structures in the NDN architecture. The authors propose a trident method to detect and mitigate SDoS attacks in underwater WSNs. In [49], a water depth aware caching and naming-based IC-WSN architecture is discussed. The proposed scheme improves the power consumption and the delay time required for underwater scenarios.

2) INFORMATION-CENTRIC INTERNET OF THINGS (IC-IoTs)

This subsection discusses the state-of-the-art research in IC-IoTs classified under the approaches based on caching, naming, routing and forwarding, mobility and other approaches.

a: APPROACHES BASED ON CACHING

A fog-based caching scheme is discussed in [50] for IC-IoT networks. The paper discusses near path and full-time caching schemes and is evaluated against traditional caching strategies to observe improvement in link load, latency, path stretch, and cache hit metrics. In the paper [51], a pre-caching strategy is discussed for IC-IoTs. The smart nodes cache the following content of the actual requested content ahead in time to improve the hop count, latency, and cache hit ratio. A caching strategy for IC-IoTs is proposed in [52]. The scheme suggests caching at leaf/edge nodes of the IoT networks based on CCN architecture. The proposed scheme improves latency, hop count, and energy efficiency comparatively. An energy-efficient and secure caching strategy for ICN-based IoT is provided in [53] named packet update caching. The work addresses the caching limitations in detail and discusses the approach to improve energy and bandwidth consumption through clustering, data purging and Incapsula CDN [54]. The authors in [55] presented distributed cache placement and popularity-based cache replacement strategies for large-scale IC-IoTs. The scheme pushes the popular content to the network edge and retains the unpopular content in the network core to improve network utilization. The collaborative cache notification and caching strategies together improve the network delay, hop count and cache utilization in IC-IOTs. A multihop cooperative caching strategy to achieve energy efficiency in IC-IoTs is proposed in [56]. The scheme discusses the tradeoff between energy-saving and delay reduction by coordinating in-network caching and sleep scheduling. The performance metrics such as energy-saving and delay reduction ratio have improved compared to the basic NDN architecture. In [57], a probabilistic cache placement and replacement policy for NDN-based IoT is discussed. The authors evaluate the frequency of requested content for content selection, neighboring nodes count for cache placement and backing up the evicted content at neighboring nodes for cache replacement. This three-step scheme maximizes the caching performance in terms of latency, cache hit and stretch ratio in NDN-based IoTs. Content popularity and distance-based caching scheme with a dynamic threshold for IC-IoTs are discussed in [58]. The scheme has been evaluated with different cache sizes for performance metrics such as delay, hop count, and cache hit ratio with improved performance. In [59], an energy-efficient cache placement scheme is proposed for IC-IoTs. The scheme performs better compared to benchmark caching strategies regarding energy saving and efficiency, and cache utilization.

b: APPROACHES BASED ON NAMING

A hybrid naming scheme for IC-IoTs is proposed in [60] by combining hierarchical and attribute-based naming methods. The paper also presents a novel concept of in-network functions for multi-source data retrieval with multiple interest packets. The authors succeeded in obtaining an improvement in lookup time and memory consumption.

c: APPROACHES BASED ON ROUTING AND FORWARDING

A reliable and efficient routing and forwarding protocol for static and mobile IC-IoTs with multiple retransmission techniques are discussed in [61]. The solution enhances the delivery rates, latency and hop count through the periodic and hysteresis-based retransmissions. In [62], an adaptive forwarding strategy is based on learning through previous data. The scheme fares well in energy efficiency, overhead, and content retrieval, with results demonstrated on NDN as IP overlay.

d: APPROACHES BASED ON MOBILITY

Producer and consumer mobility in NDN-based smart city use case is discussed in [63]. Simulations have been performed for mobile vehicular traces over NDN architecture. The evaluation results show improved network overhead and consumer satisfaction ratio during producer and consumer mobility.

e: OTHER APPROACHES

In [64], the privacy challenges of data aggregation in IC-IoTs are addressed without a trusted authority in addition to a user management scheme. The paper presents privacy and anonymity preserving protocol in IC-IoTs with low computation and communication overhead. In [65], a collaborative access control scheme for heterogeneous IC-IoTs over NDN is discussed. The scheme has shown performance improvement in terms of user latency and overhead due to the incorporation of the hierarchical key tree and modified attitude-based encryption.

As seen from the Table 5, none of the research works available in recent times provides a holistic solution for IC-WSNs/IC-IoTs. We urge the researchers to address the work in this field by considering the aspects discussed below.

- Security: Very few works addressed the threats possible in IC-WSNs/IC-IoTs and their mitigation approaches. Since the nodes are resource-constrained, threat mitigation approaches should be lightweight.
- Scalability: As the WSNs/IoTs are inherently capable of having a variable number of nodes based on their use case scenarios, scalability is an aspect to be addressed. Most of the existing works evaluated their methods with fewer nodes, but performance evaluation for a large number of nodes is essential in real-world deployments. Aspects like the effect on scalability on routing tables and data lookup time should be considered.
- Interoperability with IP: Most research focuses on clean slate ICN architecture-based implementations as its straightforward approach. For real-world deployment, a study on Interoperability with IP networks as an overlay or underlay is required.
- Cloud assistance: Cloud assistance in IC-WSNs/ IC-IoTs can bring positive effects on performance as a cloud can provide storage, analytics, reduced overhead and also as a backup in case of network fragmentation problems which is common in WSNs/IoTs.
- Mobility: As nodes in WSNs/IoTs are mobile, both producer and consumer mobility need to be evaluated in

TABLE 5. Comparision of research works in IoTs/WSNs over ICN.

Ref.	Research direction	ICN architecture	Interoperability with IP	User scalability	Add on Security	Security threat	Mitigation approaches
[44]	Information-centric big data gathering protocol for WSNs	-	×	✓	×	-	-
[45]	An architectural extension to NDN for cluster-based IC-WSNs in surveillance and monitoring use case	NDN	×	✓	×	-	-
[46]	Collaborative caching for IC-WSNs in smart campus scenario	CCNx	×	×	×	-	-
[47]	Rhythm-based user authentication scheme in IC-WSNs	-	×	×	✓	Brute attack, video and imitation attack	Convolution Neural Network, Naïve bayes classifier
[48]	Synergetic DoS attacks in underwater WSNs	NDN	×	×	✓	Interest flooding (DoS)	Trident method
[49]	Depth aware caching and naming scheme for underwater IC-WSNs	IC-WSN-water depth aware architecture	×	×	×	-	-
[50]	Fog caching strategy for IC-IoTs	-	×	×	×	-	-
[51]	Pre caching strategy for IC-IoTs	NDN	×	×	×	-	-
[52]	An edge caching strategy in IC-IoTs over CCN	CCN	×	×	×	-	-
[53]	Packet Update Caching strategy for ICN based IoTs	NDN	×	×	✓	DDoS and access control	Incapsula caching
[55]	Caching placement and replacement strategy in large scale IC-IoTs	NDN	×	✓	×	-	-
[56]	Multihop cooperative caching strategy for energy -efficient in IC-WSNs	NDN	×	×	×	-	-
[57]	Popularity aware cache placement and replacement policies in NDN based IoTs	NDN	×	×	×	-	-
[58]	Content popularity and distance based caching in IC-IoTs	CCN	×	×	×	-	-
[59]	Energy efficient and scalable caching scheme for IC-IoTs	-	×	✓	×	-	-
[60]	A hybrid naming scheme for IC-IoTs	NDN	×	✓	×	-	-
[61]	Reliable routing and forwarding protocol for Mobile IC-IoTs	CCN	×	×	×	-	-
[62]	An adaptive learning based forwarding strategy for IC-IoTs	NDN	✓	✓	×	-	-
[63]	Mobility in publish-subscribe NDN in smart cities over NDN	NDN	×	✓	×	-	-
[64]	Privacy-preserving data aggregation protocol for IC-IoTs	-	×	×	✓	Collusion, Eavesdropping	Aggregation protocol with Advanced Encryption Standard (AES) and t-out-of-n sharing algorithm
[65]	Collaborative Access control in IC-IoTs	NDN	×	×	✓	Access control	Hierarchical Key Tree naming

ICN-based works to understand the consequences and provide a practical approach to handling mobility.

3) INFORMATION-CENTRIC INDUSTRIAL IoTs

Industrial IoTs is a subclass of IoTs comprising sensors, actuators, applications and related networking equipment. The application areas span manufacturing, transportation, and industrial control systems to automotive, agriculture and energy management. The usage of ICN in IIoTs has been very promising, but the research literature available is very limited (Table 6). In this subsection, we discuss a set of works discussing Information centric IIoTs. Researchers in [93], developed a technique for adapting NDN architecture for Low-Power Wireless Personal Area Networks (LoWPAN). This technique showed performance improvements in energy consumption, latency and media utilization. A publish-subscribe-based HoP-and-Pull (HoPP) scheme for a lossy low powered IoT environment is discussed in [94]. The HoPP approach evaluated in a realistic testbed showed that the method helped with node mobility and network partitioning. In [95], the authors explored the content object security for NDN based constrained IoTs. The scheme discussed cryptographic HMAC-based methods for evaluating the security overheads at network layer level. As seen from the Table 6, the research on IIoTs with ICN paradigm is still an open and interesting area. The researchers need to further work on exhaustive study related to scalability, interoperability with IP and security.

TABLE 6. Comparision of research works in information-centric IIoTs.

Ref.	Research direction	ICN architecture	Interoperability with IP	Node Scalability	Add on Security	Security threat	Mitigation approaches
[93]	Deployment of ICN in constrained IIoTs	NDN	✓	×	×	-	-
[94]	HoPP layer on NDN to support mobility in IoTs	NDN	×	✓	×	-	-
[95]	Content object security for constrained IoTs	NDN	×	×	✓	Generic security feature	Content object security

D. VEHICULAR NETWORKING/INTERNET OF VEHICLES (IoV)

The nodes in VANETs are not concerned about the source or destination location of the information, and hence the ICN approach is apt for its deployment rather than the IP-based approach. Researchers have been studying the ICN approach in VANETs to handle dynamically changing topology, intermittent connectivity etc. The literature in the field of information-centric VANETs (IC-VANETs) is very rich, and prior to our work, there were many detailed reviews in this field. We take the opportunity to highlight the existing review of different aspects of IC-VANETs to eliminate any redundancy for the readers [66], [67], [68], [69]. Henceforth we discuss the progress in IC-VANETs research as a continuation of the prior published review articles.

1) APPROACHES BASED ON CACHING

In [70], a popularity density-based cache replacement scheme is discussed to enhance QoS. The popularity density calculation involves categorizing network traffic into its classes and then caching in dedicated sub-cache stores. In each sub cache, replacement happens based on the popularity density value, thus resulting in efficient cache utilization and network delay. A cluster-based routing method for IC-VANETs is discussed in [71], along with a cache replacement policy. The scheme improved delivery delay, hop count and slightly increased overhead. In [72], the authors studied the performance of different caching strategies in IC-VANETs. The work compares the performance metrics such as network delay, hop count and cache utilization for each caching strategy and suggests investigating intelligent caching strategies in the future. A cache node placement algorithm for heterogenous networks is presented in [73]. The scheme is proposed to improve the connectivity and quality of the communication link and improve delay, throughput and overhead. In [74], a clustering model for caching in IC-VANETS based on the vehicle trajectory is discussed. This caching model addresses the dynamic and mobility use case in VANETs and improves the metrics such as cache hit rate, hop count, delay and delivery rate. A proactive neighborhood-based caching strategy for IC-VANETs is discussed in [75]. The scheme caches the data at the left-right and front RSUs using address tables and shows performance improvement in cache utilization, hop count, and satisfied interest ratio.

In [76], a distributed blockchain-based trust mechanism in caching is provided for IC-VANETs. The scheme secures vehicle to vehicle communication through blockchain embedded in NDN architecture. The authors evaluated the scheme using metrics, cache hit ratio, hop count and malicious node detection. A game theory-based edge caching scheme is proposed in [77] for IC-VANETs. For efficient content caching, the scheme is incentive-based and provides better content access delay and reduces base station load compared to the existing caching strategies.

2) APPROACHES BASED ON ROUTING AND FORWARDING

A socially aware centrality metric-based routing scheme for IC-VANETs is proposed in [78]. The scheme identifies certain vehicles as information facilitators through the centrality ranking and enables the routing of interest and data packets through them. The authors evaluated the routing scheme for scalability and performance metrics such as interest success rate, cache hit rate and throughput. The scheme outperformed the state-of-the-art centrality-aware routing schemes. In [79], a forwarding strategy for IC-VANETs to address the broadcast storm and consumer mobility prediction problems is proposed. The scheme achieves reliable forwarding in fewer hops and interest packets. The scheme has improved interest rate, satisfied interest rate, interest satisfaction delay and hops count compared to baseline schemes available for IC-VANETs.

3) APPROACHES BASED ON MOBILITY

In [80], the source and receiver mobility handling mechanism is discussed through advertisement messages over NDN. In addition, the scheme addressed broadcast storms and network fragmentation issues in the case of mobility and showed improvements in both urban and highway VANETs usage scenarios.

4) OTHER APPROACHES

A blockchain-based secure forwarding and caching scheme is discussed in [81] for IC-VANETs. The scheme ensured trust between the nodes and secured interest and data forwarding planes in IC-VANETs by mitigating interest flooding, cache poisoning and pollution attacks.

As seen from the Table 7, none of the research works available in recent times provides a holistic solution for IC-VANETs in terms of security, mobility, caching and routing. We urge the researchers to address the work in this field by considering the aspects discussed below.

- Security: Very few works addressed the threats possible in IC-VANETs and their mitigation approaches. Since the nodes are resource-constrained, threat mitigation approaches should be lightweight.
- Scalability: In real-life scenarios, the VANETs are bound to have many vehicles/nodes. The current literature lacks a focus on node scalability, and aspects like the effect of scalability on routing tables and data lookup time should be considered.

TABLE 7. Comparision of research works in VANETs over ICN.

Ref.	Research direction	ICN architecture	Interoperabiity with IP	User scalability	Add on Security	Security threat	Mitigation approaches
[70]	Popularity density-based cache replacement scheme in VANETs	NDN	×	×	×	-	-
[71]	Cluster-based routing and a cache replacement scheme for IC-VANETs	NDN	×	×	×	-	-
[72]	Performance evaluation of in-network caching strategies for IC-VANETs	NDN	×	×	×	-	-
[73]	Cache placement algorithm for heterogeneous networks	NDN	×	✓	×	-	-
[74]	Trajectory based clustering in data caching for IC-VANETs	NDN	×	×	×	-	-
[75]	Neighborhood-based caching strategy for IC-VANETs	NDN	×	×	×	-	-
[76]	Secure cache placement strategy with trust mechanism for IC-VANETs	NDN	×	×	✓	Privacy, confidentiality	Blockchain-based approach
[77]	A game theory-based edge caching scheme for IC-VANETs	NDN	×	×	×	-	-
[78]	Centrality based routing protocol in VANETs	NDN	×	✓	×	-	-
[79]	Forwarding strategy for consumer mobility in IC-VANETs	NDN	×	×	×	-	-
[80]	Source and receiver mobility handling mechanism in IC-VANETs	NDN	×	×	×	-	-
[81]	Blockchain-based secure forwarding and caching in IC-VANETs	NDN	×	×	✓	Interest flooding, Cache pollution Cache poisoning	Blockchain-based approach

- Interoperability with IP: Again, as discussed in ICN/WSNs scenario, Most research focuses on clean slate ICN architecture-based implementations as its straightforward approach. For real-world deployment, a study on Interoperability with IP networks as an overlay or underlay is required.
- Mobility: Again, as discussed in ICN/WSNs scenario, both producer and consumer mobility need to be evaluated in ICN-based works to understand the consequences and provide a practical approach to handling mobility. The network fragmentation aspect should also be considered in this area of work.
- Heterogeneity: As VANETs are at the core of future Intelligent Transport Systems (ITS), the whole system will be heterogeneous due to different underlying wireless technologies (both legacy and modern). Hence a focus on the heterogeneity aspect is also required in future works.

E. FLYING ADHOC NETWORKS (FANETs)

Flying Adhoc Networks (FANETs) are a subclass of Mobile Adhoc networks with Unmanned Aerial Vehicles as the network nodes. FANETs find their application in disaster management, public safety insurance etc. The cooperation aware FANETs are susceptible to security attacks due to their mobility, delay and resource constraints. As the content producer location is of negligible importance in FANETs, the information-centric paradigm seems to be an excellent approach to solving IP-related issues such as mobility management, reliability and security. However, the FANETs communication does not work as-is with the inherent security (chain of trust) in ICNs due to the energy-constrained, fragmented environment (delay and overhead). Thus, the security attacks such as cache poisoning, access control and data authenticity need to be separately addressed in ICN-based FANETs. The amount of literature in this direction is minimal, and the available research on information-centric-based FANETs is discussed.

A set of trust establishment, management and data authentication schemes are proposed in [82] for ICN-based FANETs. The trust-aware scheme works well even without the GPS data in communicating UAVs. The proposed scheme improves storage, delay and computational overhead compared to the data authenticity scheme inherently present in NDN architecture. In [83], a blockchain-based approach to mitigate cache pollution attacks in UAV-assisted IC-WSNs is discussed. The scheme uses a blockchain-based caching and hash chain-based signature to mitigate cache pollution attacks. This caching method in ICN-based FANETs provides security with less overhead and energy consumption.

As seen from Table 8, the research is in its infancy, with many issues still to be addressed. Blockchain and trust-based methods seem to be reasonable security candidates for such networks. However, more research on user data privacy,

TABLE 8. Comparision of research works in FANETs over ICN.

Ref.	Research direction	ICN architecture	Interoperabiity with IP	User scalability	Add on Security	Security threat	Mitigation approaches
[82]	Trust-based communication in NDN based FANETs	NDN	×	×	✓	Interest flooding, data authentication, access control	Trust-based approach
[83]	Blockchain-based caching scheme for information -centric FANETs	NDN	×	✓	✓	Cache pollution	Blockchain and hash chain based signatures

TABLE 9. Comparision of research works in anomaly detection in content accessing over ICN.

Ref.	Research direction	ICN architecture	Interoperability with IP	Node Scalability	Add on Security	Security threat	Mitigation approaches
[88]	Architectural updates to support semantic analysis of content and anomalous content access detection	NDN	×	×	✓	Access control through Anomaly detection	Semantic content analysis

TABLE 10. Comparision of research works in information-centric social networks (IC-SNs) over ICN.

Ref.	Research direction	ICN architecture	Interoperability with IP	Node Scalability	Add on Security	Security threat	Mitigation approaches
[89]	CCN-based Virtual Private Community for social networking in mobile users	CCN	✓	×	✓	-	-
[90]	CCN-based Twitter architecture	CCN	×	×	×	-	-
[91]	CCN-based MSNs over 5G	CCN	×	×	×	-	-
[92]	Fog based Security service for IC-SNs	CCN	×	×	✓	-	Fog computing-based approach

access control, and effect due to network fragmentation is required. In addition, challenges such as scalability, interoperability with IP, network fragmentation are still unaddressed. Although ICN has shown benefits over traditional IP networks in multiple application areas, a quantitative approach to show the benefits of the ICN-based FANETs over the IP-based FANETs is required.

F. ANOMALY DETECTION IN CONTENT ACCESSING

The work in [88] proposes novel architecture updates to NDN architecture to provide semantic content analysis. The implementation is further extended to provide an anomaly content access solution in the ICN network. The work proposes semantic relationships and correlations in the content through the ndnSim simulator. The simulation results show performance improvement in delay time and detecting anomalous content requests. This work is the first of its kind and enhances the intrinsic security feature of ICN in access control mechanisms. Further research needs to be performed in this updated architecture to analyze the scalability and interoperability aspects of ICN applications(Refer Table 9).

G. INFORMATION-CENTRIC SOCIAL NETWORKS (IC-SNs)

Over the past decade, social networking applications have occupied a significant role in user's life. As content communication is at the heart of social networking and the ICN paradigm, the conglomeration of ICN and Social Networks has given rise to an application area termed Information-centric Social Networks (IC-SNs). One of the pioneer efforts in enabling social networking services to the mobile user was discussed in [89]. The researchers propose a CCN-based virtual private community (VPC) with hierarchical content naming and in-network caching. The evaluation results show that the VPC-based social networking service improves delay and load balancing in the user network. The research work in [90] evaluates how promising a solution ICN is for social networking applications. An evaluation of Twitter-based online social networks using CCN architecture is performed from both networking and user perspectives against legacy and CDN-based twitter architecture. The results showed improvements in network load from the network point of view and in QoE (Latency) from the user's point of view. A novel content-centric framework for Mobile Social Networks (MSNs) over 5G is presented in [91]. The discussed architecture consisted of mobile users, CCN nodes, and micro and macro cells. The evaluation results of the proposed social network-centric caching scheme show that the method performs better in terms of the cache hit ratio than conventional networks. In [92] the authors propose a content-aware security service for IC-SNs. This security service is based on fog computing and enhances the security in IC-SNs in addition to improvements in the cache hit ratio and network delay.

The research on IC-SNs is still in its nascency, as seen in Table 10, with much potential to replace the traditional IP-based networks. However, many experiments have not been performed to understand the implications of interoperability with IP, scalability and security aspects. Thus more work on these open research areas is required to operate the current social networks over ICN architecture fully. More quantitative approaches proving the efficiency of IC-SNs are required in upcoming research.

V. CONCLUSION

Recently, The ICN paradigm has been sought after by the research community as a solution to many current issues with

IP-based networks. Although the ICN paradigm is just over a decade old, there is a vast amount of literature available. In this article, we presented an analysis of the current state of the art in the application areas of ICN. the potential benefits of the ICN paradigm in new application areas such as social networks, FANETs, anomaly detection and Industrial IoTs are discussed. In addition, we also discussed a few of the open research challenges in each of the areas. However, each application area is different, and hence their requirements from the underlying networks are also different. In that direction, researchers need to consider the gaps and propose holistic and interoperable solutions with current IP networks.

ACKNOWLEDGMENT

The authors wish to thank the Ramaiah Institute Technology, Bengaluru, and Visvesvaraya Technological University, Belgaum, for providing the facilities and support to carry out their research works.

REFERENCES

[1] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," *IEEE Commun. Mag.*, vol. 50, no. 7, pp. 26–36, Jul. 2012.

[2] G. Carofiglio, G. Morabito, L. Muscariello, I. Solis, and M. Varvello, "From content delivery today to information centric networking," *Comput. Netw.*, vol. 57, no. 16, pp. 3116–3127, Nov. 2013.

[3] E. G. AbdAllah, H. S. Hassanein, and M. Zulkernine, "A survey of security attacks in information-centric networking," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1441–1454, 3rd Quart., 2015.

[4] *CICN*. Accessed: Apr. 12, 2022. [Online]. Available: http://www.ccnx.org/

[5] *Named Data Networking*. Accessed: Apr. 12, 2022. [Online]. Available: http://named-data.net/

[6] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in *Proc. 5th Int. Conf. Emerg. Netw. Exp. Technol.*, Rome Italy, 2009, pp. 1–12.

[7] I. Seskar, K. Nagaraja, S. Nelson, and D. Raychaudhuri, "MobilityFirst future internet architecture project," in *Proc. 7th Asian Internet Eng. Conf.*, 2011, pp. 1–3.

[8] D. Han, A. Anand, F. Dogar, B. Li, H. Lim, M. Machado, A. Mukundan, W. Wu, A. Akella, and D. G. Andersen, "XIA: Efficient support for evolvable internetworking," in *Proc. 9th USENIX Symp. Networked Syst. Design Implement. (NSDI)*, San Jose, CA, USA, 2012, pp. 309–322.

[9] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica, "A data-oriented (and beyond) network architecture," in *Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun.*, Kyoto, Japan, 2007, pp. 181–192.

[10] B. Ahlgren, M. D'Ambrosio, M. Marchisio, I. Marsh, C. Dannewitz, B. Ohlman, K. Pentikousis, O. Strandberg, R. Rembarz, and V. Vercellone, "Design considerations for a network of information," in *Proc. ACM CoNEXT Conf.*, Madrid, Spain, 2008, pp. 1–6.

[11] *PSIRP Publish-Subscribe Internet Routing Paradigm*. Accessed: Apr. 12, 2022. [Online]. Available: http://www.psirp.org/

[12] X. Qiao, H. Wang, W. Tan, A. V. Vasilakos, J. Chen, and M. B. Blake, "A survey of applications research on content-centric networking," *China Commun.*, vol. 16, no. 9, pp. 122–140, Sep. 2019.

[13] A. V. Vasilakos, Z. Li, G. Simon, and W. You, "Information centric network: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 52, pp. 1–10, Jun. 2015.

[14] D. Saxena, V. Raychoudhury, N. Suri, C. Becker, and J. Cao, "Named data networking: A survey," *Comput. Sci. Rev.*, vol. 19, pp. 15–55, Jan. 2016.

[15] R. Tourani, S. Misra, T. Mick, and G. Panwar, "Security, privacy, and access control in information-centric networking: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 566–600, 1st Quart., 2018.

[16] W. Stallings, "Introduction," in *Network Security Essentials: Applications and Standards*. London, U.K.: Pearson, 2003, p. 1.

[17] I. Moiseenko, M. Stapp, and D. Oran, "Communication patterns for web interaction in named data networking," in *Proc. 1st Int. Conf. Inf.-Centric Netw.*, Paris, France, 2014, pp. 87–96.

[18] G. Nan, X. Qiao, Y. Tu, W. Tan, L. Guo, and J. Chen, "Design and implementation: The native web browser and server for content-centric networking," in *Proc. ACM Conf. Special Interest Group Data Commun.*, London, U.K., Aug. 2015, pp. 609–610.

[19] X. Qiao, P. Ren, J. Chen, W. Tan, M. B. Blake, and W. Xu, "Session persistence for dynamic web applications in named data networking," *J. Netw. Comput. Appl.*, vol. 125, pp. 220–235, Jan. 2019.

[20] M. Sardara, "Towards a scalable and programmable incremental deployment of ICN in the real world," Ph.D. dissertation, Univ. Paris-Saclay, Paris, France, 2019.

[21] M. Jahanian, J. Chen, and K. K. Ramakrishnan, "Managing the evolution to future internet architectures and seamless interoperation," in *Proc. 29th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Honolulu, HI, USA, Aug. 2020, pp. 1–11.

[22] (Apr. 14, 2022). *Characteristics of Modern Web Applications*. Accessed: Apr. 2022. [Online]. Available: https://docs.microsoft.com/en-us/dotnet/architecture/modern-web-apps-azure/modern-web-applications-characteristics

[23] B. Ahlgren, A. Jonasson, and B. Ohlman, "Demo overview: HTTP live streaming over NetInf transport," in *Proc. 1st Int. Conf. Inf.-Centric Netw.*, 2014, pp. 203–204.

[24] S. Lederer, C. Mueller, C. Timmerer, and H. Hellwagner, "Adaptive multimedia streaming in information-centric networks," *IEEE Netw.*, vol. 28, no. 6, pp. 91–96, Nov. 2014.

[25] S. Petrangeli, N. Bouten, M. Claeys, and F. De Turck, "Towards SVC-based adaptive streaming in information centric networks," in *Proc. IEEE Int. Conf. Multimedia Expo Workshops (ICMEW)*, Turin, Italy, Jun. 2015, pp. 1–6.

[26] C. Westphal, S. Lederer, D. Posch, C. Timmerer, A. Azgin, W. Liu, C. Mueller, A. Detti, D. Corujo and J. Wang, "Adaptive video streaming over information-centric networking (ICN)," IRTF, Tech. Rep. RFC 7933, 2016.

[27] M. C. Group. *ITEC—Dynamic Adaptive Streaming Over HTTP*. DASH Research at the Institute of Information Technology. Alpen-Adria Universitaet Klagenfurt. Accessed: Apr. 2022. [Online]. Available: https://dash.itec.aau.at/

[28] B. Rainer, D. Posch, and H. Hellwagner, "Investigating the performance of pull-based dynamic adaptive streaming in NDN," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 8, pp. 2130–2140, Aug. 2016.

[29] J. Saltarin, E. Bourtsoulatze, N. Thomos, and T. Braun, "Adaptive video streaming with network coding enabled named data networking," *IEEE Trans. Multimedia*, vol. 19, no. 10, pp. 2182–2196, Oct. 2017.

[30] C. Xu, W. Quan, A. V. Vasilakos, H. Zhang, and G.-M. Muntean, "Information-centric cost-efficient optimization for multimedia content delivery in mobile vehicular networks," *Comput. Commun.*, vol. 99, pp. 93–106, Feb. 2017.

[31] R. Nakagawa, S. Ohzahata, R. Yamamoto, and T. Kato, "A congestion avoidance for adaptive streaming over ICN using bitrate feedback from in-network nodes," in *Proc. 7th Int. Symp. Comput. Netw. Workshops (CANDARW)*, Nagasaki, Japan, Nov. 2019, pp. 40–46.

[32] A. Tagami, K. Ueda, R. Lukita, J. De Benedetto, M. Arumaithurai, G. Rossi, A. Detti, and T. Hasegawa, "Tile-based panoramic live video streaming on ICN," in *Proc. IEEE Int. Conf. Commun. Workshops*, Shanghai, China, May 2019, pp. 1–6.

[33] W. Liu, G. Zhang, and Q. Gao, "Coupling DAS, SVC and NDN: An SVC-aware cache and forwarding policy for NDN routers," in *Proc. 1st IEEE Int. Conf. Hot Inf.-Centric Netw. (HotICN)*, Shenzhen, China, Aug. 2018, pp. 1–6.

[34] W. Li, S. M. A. Oteafy, M. Fayed, and H. S. Hassanein, "Bitrate adaptation-aware cache partitioning for video streaming over information-centric networks," in *Proc. IEEE 43rd Conf. Local Comput. Netw. (LCN)*, Chicago, IL, USA, Oct. 2018, pp. 401–408.

[35] M. Rayani, R. H. Glitho, and H. Elbiaze, "ETSI multi-access edge computing for dynamic adaptive streaming in information centric networks," in *Proc. IEEE Global Commun. Conf.*, Taipei, Taiwan, Dec. 2020, pp. 1–6.

[36] F. Wu, W. Yang, J. Ren, F. Lyu, X. Ding, and Y. Zhang, "Adaptive video streaming using dynamic NDN multicast in WLAN," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Toronto, ON, Canada, Jul. 2020, pp. 97–102.

[37] W. Liu, G. Zhang, and Q. Gao, "SVC-aware cache coordination schemes for dynamic adaptive streaming in named data networking," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Dublin, Ireland, Jun. 2020, pp. 1–6.

[38] R. Nakagawa, S. Ohzahata, R. Yamamoto, and T. Kato, "Mitigating congestion with explicit cache placement notification for adaptive video streaming over ICN," *IEICE Trans. Inf. Syst.*, vol. 104, no. 9, pp. 1406–1419, 2021.

[39] I. U. Din, H. Asmat, and M. Guizani, "A review of information centric network-based Internet of Things: Communication architectures, design issues, and research opportunities," *Multimedia Tools Appl.*, vol. 78, no. 21, pp. 30241–30256, Nov. 2019.

[40] S. Arshad, M. A. Azam, M. H. Rehmani, and J. Loo, "Recent advances in information-centric networking-based Internet of Things (ICN-IoT)," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2128–2158, Oct. 2017.

[41] B. Nour, K. Sharif, F. Li, S. Biswas, H. Moungla, M. Guizani, and Y. Wang, "A survey of Internet of Things communication using ICN: A use case perspective," *Comput. Commun.*, vols. 142–143, pp. 95–123, Jun. 2019.

[42] B. Nour, K. Sharif, F. Li, and Y. Wang, "Security and privacy challenges in information-centric wireless Internet of Things networks," *IEEE Secur. Privacy*, vol. 18, no. 2, pp. 35–45, Mar. 2020.

[43] A. Djama, B. Djamaa, and M. R. Senouci, "Information-centric networking solutions for the Internet of Things: A systematic mapping review," *Comput. Commun.*, vol. 159, pp. 37–59, Jun. 2020.

[44] R. Lachowski, M. Pellenz, E. Jamhour, M. Penna, G. Brante, G. Moritz, and R. Souza, "ICENET: An information centric protocol for big data wireless sensor networks," *Sensors*, vol. 19, no. 4, p. 930, Feb. 2019.

[45] M. A. U. Rehman, R. Ullah, B.-S. Kim, B. Nour, and S. Mastorakis, "CCIC-WSN: An architecture for single-channel cluster-based information-centric wireless sensor networks," *IEEE Internet Things J.*, vol. 8, no. 9, pp. 7661–7675, May 2021.

[46] G. Jaber and R. Kacimi, "A collaborative caching strategy for content-centric enabled wireless sensor networks," *Comput. Commun.*, vol. 159, pp. 60–70, Jun. 2020.

[47] H. Bi, Y. Sun, J. Liu, and L. Cao, "SmartEar: Rhythm-based tap authentication using earphone in information-centric wireless sensor network," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 885–896, Jan. 2022.

[48] Y. Li, Y. Liu, Y. Wang, Z. Guo, H. Yin, and H. Teng, "Synergetic denial-of-service attacks and defense in underwater named data networking," in *Proc. IEEE Conf. Comput. Commun.*, Toronto, ON, Canada, Jul. 2020, pp. 1569–1578.

[49] J. Li, J. Wu, C. Li, W. Yang, A. K. Bashir, J. Li, and Y. D. Al-Otaibi, "Information-centric wireless sensor networking scheme with water-depth-awareness content caching for underwater IoT," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 858–867, Jan. 2022.

[50] Y. Hua, L. Guan, and K. G. Kyriakopoulos, "A fog caching scheme enabled by ICN for IoT environments," *Future Gener. Comput. Syst.*, vol. 111, pp. 82–95, Oct. 2020.

[51] M. Zhang, B. Hao, R. Wang, and Y. Wang, "A pre-caching strategy based on the content relevance of smart device's request in information-centric IoT," *IEEE Access*, vol. 8, pp. 75761–75771, 2020.

[52] H. Asmat, I. U. Din, F. Ullah, M. Talha, M. Khan, and M. Guizani, "ELC: Edge linked caching for content updating in information-centric Internet of Things," *Comput. Commun.*, vol. 156, pp. 174–182, Apr. 2020.

[53] I. U. Din, S. Hassan, A. Almogren, F. Ayub, and M. Guizani, "PUC: Packet update caching for energy efficient IoT-based information-centric networking," *Future Gener. Comput. Syst.*, vol. 111, pp. 634–643, Oct. 2020.

[54] *Incapsula*. Accessed: 2022. [Online]. Available: https://www.cdnoverview.com/cdn/incapsula/

[55] B. Nour, H. Khelifi, H. Moungla, R. Hussain, and N. Guizani, "A distributed cache placement scheme for large-scale information-centric networking," *IEEE Netw.*, vol. 34, no. 6, pp. 126–132, Nov. 2020.

[56] Y. Yang and T. Song, "Energy-efficient cooperative caching for information-centric wireless sensor networking," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 846–857, Jan. 2022.

[57] 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.

[58] S. Kumar and R. Tiwari, "Dynamic popularity window and distance-based efficient caching for fast content delivery applications in CCN," *Eng. Sci. Technol., Int. J.*, vol. 24, no. 3, pp. 829–837, Jun. 2021.

[59] O. Serhane, K. Yahyaoui, B. Nour, and H. Moungla, "Energy-aware cache placement scheme for IoT-based ICN networks," in *Proc. IEEE Int. Conf. Commun.*, Montreal, QC, Canada, Jun. 2021, pp. 1–6.

[60] B. Nour, K. Sharif, F. Li, H. Moungla, and Y. Liu, "A unified hybrid information-centric naming scheme for IoT applications," *Comput. Commun.*, vol. 150, pp. 103–114, Jan. 2020.

[61] E. Borgia, R. Bruno, and A. Passarella, "Reliable data delivery in ICN-IoT environments," *Future Gener. Comput. Syst.*, vol. 134, pp. 271–286, Sep. 2022.

[62] A. Djama, B. Djamaa, M. R. Senouci, and N. Khemache, "LAFS: A learning-based adaptive forwarding strategy for NDN-based IoT networks," *Ann. Telecommun.*, vol. 77, pp. 1–20, Jul. 2021.

[63] D. Hernandez, L. Gameiro, C. Senna, M. Luis, and S. Sargento, "Handling producer and consumer mobility in IoT publish–subscribe named data networks," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 868–884, Jan. 2022.

[64] C. Xu, L. Zhang, L. Zhu, C. Zhang, X. Du, M. Guizani, and K. Sharif, "Aggregate in my way: Privacy-preserving data aggregation without trusted authority in ICN," *Future Gener. Comput. Syst.*, vol. 111, pp. 107–116, Oct. 2020.

[65] B. Chen, L. Liu, and H. Ma, "HAC: Enable high efficient access control for information-centric Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10347–10360, Oct. 2020.

[66] 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.

[67] 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.

[68] M. Amadeo, "A literature review on caching transient contents in vehicular named data networking," *Telecom*, vol. 2, no. 1, pp. 75–92, Feb. 2021.

[69] M. Safwat, A. Elgammal, E. G. Abdallah, and M. A. Azer, "Survey and taxonomy of information-centric vehicular networking security attacks," *Ad Hoc Netw.*, vol. 124, Jan. 2022, Art. no. 102696.

[70] H. Khelifi, S. Luo, B. Nour, and H. Moungla, "A QoS-aware cache replacement policy for vehicular named data networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Waikoloa, HI, USA, Dec. 2019, pp. 1–6.

[71] J. Thaenthong and S. Chootong, "Enhanced data dissemination for vehicular content-centric networking (VCCN) using cluster maintenance system," *Sci., Eng. Health Stud.*, vol. 2021, Dec. 2021, Art. no. 21040006.

[72] H. Khelifi, S. Luo, B. Nour, and H. Moungla, "In-network caching in ICN-based vehicular networks: Effectiveness & performance evaluation," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Dublin, Ireland, Jun. 2020, pp. 1–6.

[73] T. Abar, A. Rachedi, A. B. Letaifa, P. Fabian, and S. E. Asmi, "FellowMe cache: Fog computing approach to enhance (QoE) in Internet of Vehicles," *Future Gener. Comput. Syst.*, vol. 113, pp. 170–182, Dec. 2020.

[74] 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.

[75] I. U. Din, B. Ahmad, A. Almogren, H. Almajed, I. Mohiuddin, and J. J. P. C. Rodrigues, "Left-right-front caching strategy for vehicular networks in ICN-based Internet of Things," *IEEE Access*, vol. 9, pp. 595–605, 2021.

[76] Q. Saleem, I. U. Din, A. Almogren, I. Alkhalifa, H. A. Khattak, and J. J. P. C. Rodrigues, "Named data networking-based on-demand secure vehicle-to-vehicle communications," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–15, Nov. 2021.

[77] C. Wang, C. Chen, Q. Pei, N. Lv, and H. Song, "Popularity incentive caching for vehicular named data networking," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 4, pp. 3640–3653, Apr. 2022.

[78] J. A. Khan and Y. Ghamri-Doudane, "STRIVE: Socially-aware three-tier routing in information-centric vehicular environment," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Washington, DC, USA, Dec. 2016, pp. 1–7.

[79] 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.*, Taipei, Taiwan, Dec. 2020, pp. 1–6.

[80] J. M. Duarte, T. Braun, and L. A. Villas, "MobiVNDN: A distributed framework to support mobility in vehicular named-data networking," *Ad Hoc Netw.*, vol. 82, pp. 77–90, Jan. 2019.

[81] H. Khelifi, S. Luo, B. Nour, H. Moungla, S. H. Ahmed, and M. Guizani, "A blockchain-based architecture for secure vehicular named data networks," *Comput. Electr. Eng.*, vol. 86, Sep. 2020, Art. no. 106715.

[82] 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.

[83] S. Mori, "Secure caching scheme using blockchains for unmanned aerial vehicle-assisted information-centric wireless sensor networks," *J. Signal Process.*, vol. 26, no. 1, pp. 21–31, 2022.

[84] C. Safitri, R. Mandala, Q. N. Nguyen, and T. Sato, "Artificial intelligence approach for name classification in information-centric networking-based Internet of Things," in *Proc. IEEE Int. Conf. Sustain. Eng. Creative Comput. (ICSECC)*, Dec. 2020, pp. 158–163.

[85] K. Yao, Z. Li, L. Yao, and K. Lang, "Popularity prediction caching based on logistic regression in vehicular content centric networks," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 35, no. 3, pp. 150–161, 2020.

[86] O. A. Khan, M. A. Shah, I. U. Din, B.-S. Kim, H. A. Khattak, J. J. Rodrigues, H. Farman, and B. Jan, "Leveraging named data networking for fragmented networks in smart metropolitan cities," *IEEE Access*, vol. 6, pp. 75899–75911, 2018.

[87] E. Mannes and C. Maziero, "Naming content on the network layer: A security analysis of the information-centric network model," *ACM Comput. Surv.*, vol. 52, no. 3, pp. 1–28, May 2020.

[88] M. Xi, J. Wu, J. Li, and G. Li, "Sema-ICN: Toward semantic information-centric networking supporting smart anomalous access detection," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.

[89] J. Kim, M.-W. Jang, B.-J. Lee, and K. Kim, "Content centric network-based virtual private community," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2011, pp. 843–844.

[90] B. Mathieu, P. Truong, W. You, and J. F. Peltier, "Information-centric networking: A natural design for social network applications," *IEEE Commun. Mag.*, vol. 50, no. 7, pp. 44–51, Jul. 2012.

[91] Z. Su and Q. Xu, "Content distribution over content centric mobile social networks in 5G," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 66–72, Jun. 2015.

[92] J. Wu, M. Dong, K. Ota, J. Li, and Z. Guan, "FCSS: Fog-computing-based content-aware filtering for security services in information-centric social networks," *IEEE Trans. Emerg. Topics Comput.*, vol. 7, no. 4, pp. 553–564, Oct. 2019.

[93] 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.

[94] C. Gündoğan, P. Kietzmann, T. C. Schmidt, and M. Wählisch, "A mobility-compliant publish–subscribe system for an information-centric Internet of Things," *Comput. Netw.*, vol. 203, Feb. 2022, Art. no. 108656.

[95] 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.

[96] M. Ambrosin, A. Compagno, M. Conti, C. Ghali, and G. Tsudik, "Security and privacy analysis of national science foundation future Internet architectures," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1418–1442, 2nd Quart., 2018.

[97] D. Page, "Defending against cache-based side-channel attacks," *Inf. Secur. Tech. Rep.*, vol. 8, no. 1, pp. 30–44, Mar. 2003.

LALITHA CHINMAYEE M. HURALI received the B.E. degree from the RV College of Engineering, Bengaluru, India, in 2015, and the M.Tech. degree from the Ramaiah Institute of Technology, Bengaluru, in 2020, where she is currently pursuing the Ph.D. degree with the Department of Computer Science and Engineering under Ramaiah Doctoral Fellowship. Her research interests include information-centric networks, network security, network management, vehicular ad hoc networks, and machine learning.

ANNAPURNA P. PATIL (Senior Member, IEEE) received the Ph.D. degree from Visvesvaraya Technological University (VTU), Belgaum, Karnataka, India, in 2014. She is currently a Professor and the Head of the Department of Computer Science and Engineering, Ramaiah Institute of Technology (RIT), Bengaluru. She has several publications in reputed conferences and journals. She is involved in collaborative works with CISCO, IBM, HPE, Nihon Communications Ltd., and Samsung, Bengaluru, for various research projects. Her research interests include mobile ad hoc networks, protocol engineering, artificial intelligence, data analytics, and distributed computing. She is an IETE Fellow, a LMCSI, a LMISTE, and an ACM Member, and held the position of a Chair of the IEEE WIE, Bengaluru Section, in 2018.