Access Control Mechanisms in Named Data Networks: A Comprehensive Survey

Boubakr Nour, Hakima Khelifi, Rasheed Hussain, Spyridon Mastorakis, Hassine Moungla

Access Control Mechanisms in Named Data Networks: A Comprehensive Survey

BOUBAKR NOUR, Beijing Institute of Technology, China
HAKIMA KHELIFI, Beijing Institute of Technology, China
RASHEED HUSSAIN, Innopolis University, Russia
SPYRIDON MASTORAKIS, University of Nebraska Omaha, USA
HASSINE MOUNGLA, Université de Paris, France

Information-Centric Networking (ICN) has recently emerged as a prominent candidate for the Future Internet Architecture (FIA) that addresses existing issues with the host-centric communication model of the current TCP/IP-based Internet. Named Data Networking (NDN) is one of the most recent and active ICN architectures that provides a clean slate approach for Internet communication. NDN provides intrinsic content security where security is directly provided to the content instead of communication channel. Among other security aspects, Access Control (AC) rules specify the privileges for the entities that can access the content. In TCP/IP-based AC systems, due to the client-server communication model, the servers control which client can access a particular content. In contrast, ICN-based networks use content names to drive communication and decouple the content from its original location. This phenomenon leads to the loss of control over the content causing different challenges for the realization of efficient AC mechanisms. To date, considerable efforts have been made to develop various AC mechanisms in NDN. In this paper, we provide a detailed and comprehensive survey of the AC mechanisms in NDN. We follow a holistic approach towards AC in NDN where we first summarize the ICN paradigm, describe the changes from channel-based security to content-based security and highlight different cryptographic algorithms and security protocols in NDN. We then classify the existing AC mechanisms into two main categories: *Encryption-based AC* and *Encryption-independent AC*. Each category has different classes based on the working principle of AC (*e.g.,* Attribute-based AC, Name-based AC, Identity-based AC, etc). Finally, we present the lessons learned from the existing AC mechanisms and identify the challenges of NDN-based AC at large, highlighting future research directions for the community.

CCS Concepts: • **Networks** → **Network design principles**; **Security protocols**.

Additional Key Words and Phrases: Information-Centric Networking, Named Data Networking, Access Control Mechanisms, Survey

ACM Reference Format:
Boubakr Nour, Hakima Khelifi, Rasheed Hussain, Spyridon Mastorakis, and Hassine Moungla. 2020. Access Control Mechanisms in Named Data Networks: A Comprehensive Survey. 1, 1 (December 2020), 32 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

The current Internet ecosystem has been designed to achieve end-to-end communication between two known devices. Accordingly, each device is assigned an unique Internet Protocol (IP) address to allow communication and resources sharing. The current Internet follows the host-centric model, where the communication is based upon, among other factors, the address of the destination node. This model has been adopted as the main communication paradigm over years, where resource sharing between two devices was required. However, today's Internet is

Authors' addresses: Boubakr Nour, n.boubakr@ieee.org, Beijing Institute of Technology, Beijing, China; Hakima Khelifi, hakima@bit.edu.cn, Beijing Institute of Technology, Beijing, China; Rasheed Hussain, r.hussain@innopolis.ru, Innopolis University, Innopolis, Russia; Spyridon Mastorakis, smastorakis@unomaha.edu, University of Nebraska Omaha, Omaha, USA; Hassine Moungla, hassine.moungla@parisdescartes.fr, Université de Paris, Paris, France.

2020. XXXX-XXXX/2020/12-ART $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

witnessing a tremendous growth in connected devices and major changes in the application design [130], which affect the end-user requirements. To address these changes, the IP stack has been refined with add-ons and protocols to support various features. However, TCP/IP became a complex network architecture by adding extra patches to support security, mobility, and management.

To meet the user demands and address the changes in the nature of applications, various solutions have been proposed to realize Future Internet Architectures (FIA) [113]. The current Internet model is shifting from the host-based communication toward the content-oriented model [23]. End-users are inherently interested in what they request and consume regardless of who is offering the content or service. This vision of communication is known as Information-Centric Networking (ICN) [28, 49, 156].

In contrast to the host-centric model, where an IP address is used to deliver packets to the destination host, ICN uses the content name to drive the communication and fetch the content from the network [10]. Various ICN projects have been proposed as part of FIA including Data Oriented Network (DONA) [62], Scalable and Adaptive Internet Solutions (4WARD/SAIL) [1, 2], Publish-Subscribe Internet Routing Paradigm (PSIRP/PURSUIT) [33], Content-Centric Networking (CCN) [111], COMET [37], CONVERGENCE [92], MobilityFirst [125], and Named-Data Networking (NDN) [161]. We refer interested readers to other surveys [6, 156] for more details. In this work, we focus on research relevant to NDN, since it has received considerable attention from the research community among various FIA proposals and it continues to be favored as the most prominent FIA candidate.

In a nutshell, NDN [162] identifies the content using semantically meaningful, hierarchical names. NDN decouples the content from its original location and enables in-network caching. Intermediate nodes have the ability to cache content and fulfill future demands [122, 144]. NDN offers a receiver-driven communication model based on the exchange of interest-Data packets. A content consumer initiates a request in the form of an *interest* packet that carries the requested content name. Intermediate nodes forward the requests based on that name using name-based forwarding rules. When the request reaches a content provider/producer or a content store that can offer the requested content, a reply is sent out in the form of a *Data* packet.

NDN features a content-based security model [39, 149, 159, 165], since each Data packet is cryptographically signed by the entity that produced it. In contrast to host-based networks, where communication security relies on the security of the communication channel itself, NDN directly secures the content exchanged over the network regardless of the used communication channel. All security-related information is bound to the content and stays with the content during transmission over the network and at rest (e.g., when cached in the content store of intermediate nodes). Although this concept is promising in terms of securing content at the publishing phase, various issues may arise regarding efficiency and scalability, the used security algorithms, and privacy [96].

Access Control (AC) [145] is a vital aspect of today's Internet, since it determines who can access what content. Existing TCP/IP-based AC systems are heavily influenced by the client-server communication model. The request is sent to the service/content provider or a delegated server who has a list of access rules–based on this list, the privileged access is determined. This AC model contradicts the NDN communication model, where content can be cached in the network and can be retrieved from any entity that can provide it, being fundamentally different than the existing client-server communication model.

Various efforts have been conducted by the research community to explore AC mechanisms for NDN. Some solutions take the communication back to a client-server model by enforcing the consumer to communicate with the original producer to get authenticated through access rules. However, this concept ignores the advantages of ubiquitous in-network caching and may fail due to producer's unavailability. Other solutions take advantage of NDN naming, introducing Name-based Access Control (NAC) [158]. Between the former and the latter solutions, hybrid solutions have also been proposed.

Overall, AC solutions offer the means for secure content dissemination and privileged access in NDN. Motivated by the significance of access control as a problem, in this work, we provide a comprehensive survey on the existing AC schemes in NDN.

Table 1. Comparison of contributions among related surveys.

Ref.	Year	AC Mechanisms	Recent Work	Research Challenges	Future Direction	Limitation	Covered AC Sol.	Covered Year
[4]	2015	✓	✗	✓	✗	• Broader security attack analysis. • Targeting several ICN architectures. • Not specialized on Named Data Networking.	1	2012
[9]	2018	✗	✗	✓	✓	• No review of technical solutions. • Broader security and privacy analysis. • Targeting several ICN architectures. • Not specialized on Named Data Networking. • Not specialized on access control.	NA	NA
[137]	2018	✓	✗	✗	✓	• Focus on security, privacy, and access control. • Targeting several ICN architectures. • Not specialized on Named Data Networking.	19	2009-2017
[76]	2016	✗	✗	✓	✓	• No review of technical solutions. • Not specialized on access control.	NA	NA
[40]	2017	✗	✗	✓	✓	• Focus on privacy in CCN networks. • Not specialized on access control.	NA	NA
[16]	2018	✗	✗	✓	✓	• Focus on security attacks in vehicular cyber-physical systems. • No review of technical solutions. • Not specialized on access control.	NA	NA
[61]	2018	✗	✗	✓	✓	• Focus on security and privacy in vehicular named networks. • Not specialized on access control.	NA	NA
Our	2019	✓	✓	✓	✓	/	28	2009-2019

1.1 Related Surveys

Different surveys have been published regarding ICN and/or NDN, focusing on the general architecture [6, 121, 143], specific components/features [5, 10, 27, 127, 142, 160], or well-defined applications and use cases [58, 102]. However, there is a lack of surveys that are targeting access control in NDN. To justify the need and contribution of this survey, we summarize the existing surveys in Table 1.

Ambrosin *et al.* [9] provide analysis on security and privacy features in Future Internet architectures designed by the U.S. National Science Foundation (NSF) including Nebula, MobilityFirst, Named Data Networking, and eXpressive Internet Architecture. Tourani *et al.* [137] reviewed the security and privacy issues in ICN. The authors also covered access control schemes, but in a rather high-level manner, without focusing on the NDN architecture. Finally, they classified the existing solutions according to features such as naming, routing, caching, etc. Similarly, Abdallah *et al.* [4] survey security attacks that are related to ICN implementations or may have impact to ICN features. In this study, they classified the existing attacks based on ICN aspects (i.e. naming-related attacks, routing-elated attacks, caching and other related attacks). The authors also discussed the security requirements to provide confidentiality, integrity, availability, and privacy. However, the authors did not cover access control solutions. Lutz *et al.* [76] compare the CCN communication model with the current Internet model from the security and privacy point-of-view. The authors also present the security and privacy benefits of CCN, such as verifiable integrity, absence of device addressing, and protection against DoS attacks. Although they discuss some of the existing challenges and provide research directions, the authors do not offer a comprehensive survey on the existing security solutions and do not cover the access control aspect. Similarly, Ghali *et al.* [40] assess

the privacy of CCN. The authors discuss the existing privacy attacks and evaluate them using a custom CCN simulator.

On the other hand, Bouk *et al.* [16] discuss the security attacks and vulnerabilities in vehicular cyber-physical systems, and highlight a bunch of issues and challenges. Based on this study, the authors introduce an NDN-based cyber-resilient architecture to detect attacks and provide a resilience system. However, the authors did not cover access control aspects either in their study or in the proposed architecture. Similarly, Khelifi *et al.* [61] review the existing vehicular network attacks and classify them based on an NDN point-of-view. The authors identify various issues and challenges that require future investigation by the research community. However, the work targets vehicular environments without providing details about access control.

Besides the aforementioned survey and study efforts, *Information-Centric Networking Research Group* (ICNRG) – an IRTF research group provides a set of RFCs and drafts on ICN and its applicability. In particular, RFC 7927 [66] describes the challenges and issues of ICN before being widely deployed on core networks. RFC 7945 [114] provides an overview of the existing tools to evaluate ICN network focusing on the security aspects (e.g., authentication, authorization, access control, and logging), while ICN deployment guidelines have been provided to the broader community [116].

1.2 Motivation and Main Contributions

Contrary to existing surveys, our work focuses on access control solutions in NDN. In comparison to [137] (where authors study security, privacy, and access control from a bird's eye view), we thoroughly investigate and review the existing access control schemes in ICN/NDN[1]. We further classify existing solutions into two broad categories, and then each category into a set of sub-categories.

In this regard, the major contributions of our work are the following:

- We review content-based security, cryptographic algorithms and security protocols, and access control in NDN.
- We provide a comprehensive survey of the access control schemes (both encryption-based and encryption independent solutions) in NDN.
- We identify future challenges and research directions for access control in NDN.

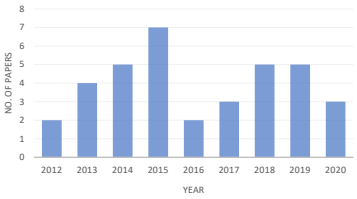
1.3 Methodology of Survey on Access Control Mechanisms in Named Data Networking

In the following, we present the methodology that we utilized to survey access control mechanisms in NDN [29]. We also present the taxonomy of existing literature.

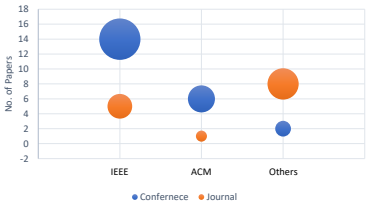
Adopted Methodology. To present a comprehensive survey of the state-of-the-art on access control mechanisms in NDN, we have adopted a systematic survey methodology. This methodology aims to provide a holistic overview described in the following steps:

- **Surveyed Databases:** To achieve our objective, we have collected various published papers up to June 2020 available on domain-relevant electronic databases, including *ACM Digital Library*, *IEEE Xplore*, *Science Direct*, and *Springer Link*. Furthermore, we have collected articles related to this domain from *arXiv*, *Hindawi*, *MDPI*, and *Google Scholar* databases, as well as standardization research work from various *IETF* working groups.
- **Targeted topic:** In our work, the targeted topic was "*Access Control in Named Data Networking*".
- **Search strings:** We adopted an automated search process and used the following keywords for our search: ("*All Metadata*": "*Access Control Mechanism*" AND ("*Named Data Networking*" OR "*Content-Centric Networking*")).

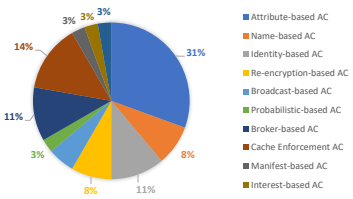
[1]Without loss of generality, we use the terms 'ICN', 'NDN', and 'CCN' interchangeably in this survey.



(a) Papers published per year.



(b) Distribution of collected papers per database.



(c) Distribution of research papers per access control category.

Fig. 1. Statistic on collected papers.

- **Filtering:** The filtering phase was separated into two steps: (i) we analyzed information related to each paper's metadata, such as title, abstract, and keywords; and (ii) we performed a full analysis of the paper.
- **Selection criteria:** This phase consisted of evaluating the papers retained from the previous phase by keeping only relevant papers and excluding those which are irrelevant, duplicated, and/or not written in English. The considered *Inclusion Criteria* (IC) were: research papers focusing on the access control in NDN; while the considered *Exclusion Criteria* (EC) were: papers that do not address access control in NDN as their main contribution as well as those consisting solely of bibliography, table of contents, references and keynote talks, editorial articles, or summaries of conferences.
- **Research Questions (RQ):** For the retained papers, the following questions were considered: RQ1 – How are the publications related to access control in NDN distributed over the years?, RQ2 – Which are the major journals and conferences that publish articles about access control in NDN?
  In response to RQ1, Fig. 1a shows that the research community started exploring access control solutions in NDN around 2012 (CCN was proposed in 2009 and NDN in 2010). Since then, the curve has taken an ascending trend. In 2016, fewer papers were published on the topic, but then researchers started concentrating on access control again as NDN was adopted as the communication enabler for different use-cases. These statistics confirm the relevance of the topic, which increasingly gains ground and interest within the research community. In response to RQ2, the bubble plot of Fig. 1b summarizes the distribution of the collected papers per publication type (journal or conference) and database (ACM, IEEE, or other publishers).

Taxonomy of the Reviewed Literature. A high-level analysis of the collected articles in the literature focusing on access control in NDN can be classified into two main categories: *Encryption-based Access Control* and *Encryption-independent Access Control*. Each category has a set of sub-categories. Figure 1c shows the distribution of research papers.

1.4 Survey Structure

The rest of this survey is organized as illustrated in Figure 2 and described as follows. Section 2 introduces ICN and its features, as well as presents an overview of NDN. Section 3 discusses the communication security in ICN and the shift from channel-based security towards content-based security, presents the existing cryptographic algorithms and security protocols in NDN, and introduces the access-control concept as well as highlights the required security service. Section 4 reviews the existing encryption-based access control. Similarly, Section 5 presents a review on encryption independent access control. Section 6 presents challenges and highlights different guidelines and future research directions. Finally, Section 7 concludes the survey.

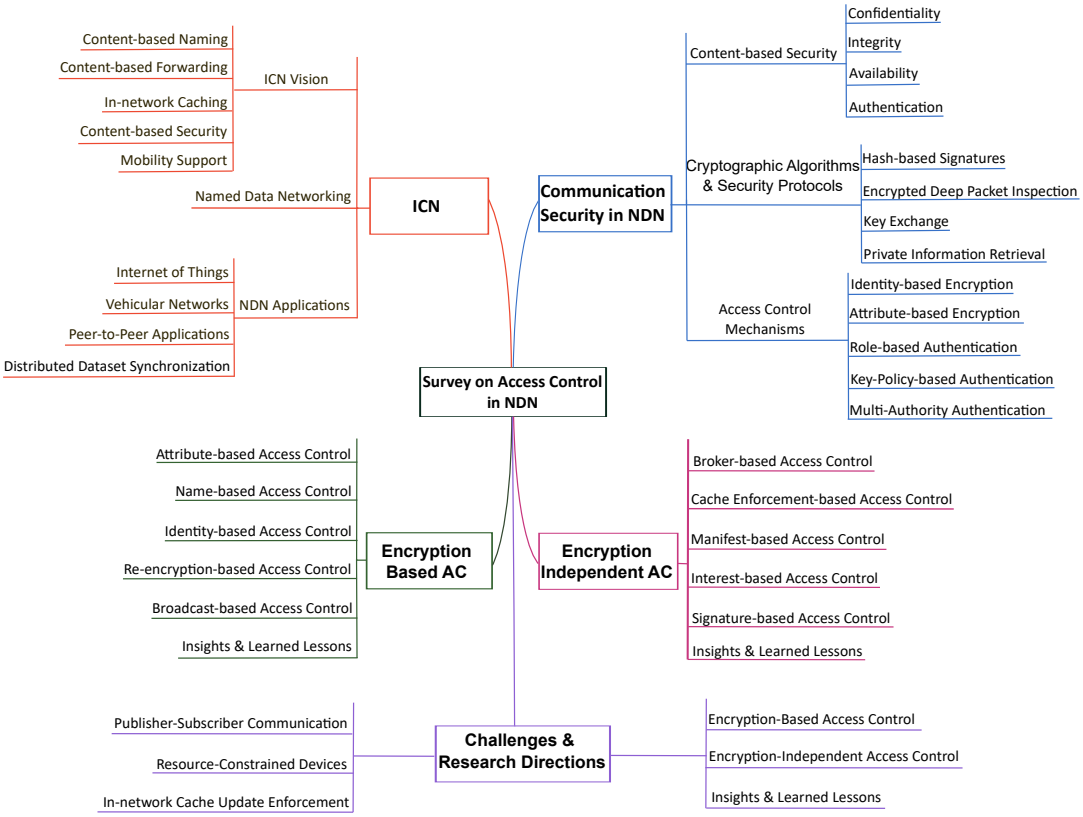


Fig. 2. Structure of the paper and taxonomy.

2 INFORMATION-CENTRIC NETWORK: A BIRD'S EYE VIEW

Information-Centric Networking [6] has been proposed as an alternative network architecture to address the major challenges in the existing IP-based network including routing, content sharing, scalability, and security. In the following, we provide an overview on ICN highlighting its global vision. Then, we present NDN architecture and its working principles as well as NDN applications.

2.1 ICN Vision

The ICN paradigm transforms the way the current Internet functions by leveraging content naming as the communication cornerstone, thus, replacing the current host-centric communication model [146]. Figure 3 illustrates the basic communication model in ICN that includes a content producer (original publisher), intermediate routers with caching capabilities, consumers, and edge servers. We present an overview of the main ICN features below.

2.1.1 Content-based Naming. The content name [106, 107] is the essential element in ICN. A name is used by the network as the content identifier, while it should also be persistent to validate the content. The used naming scheme must be scalable and allow for name aggregation and fast lookup performance. Four main types of naming schemes have been proposed in ICN:

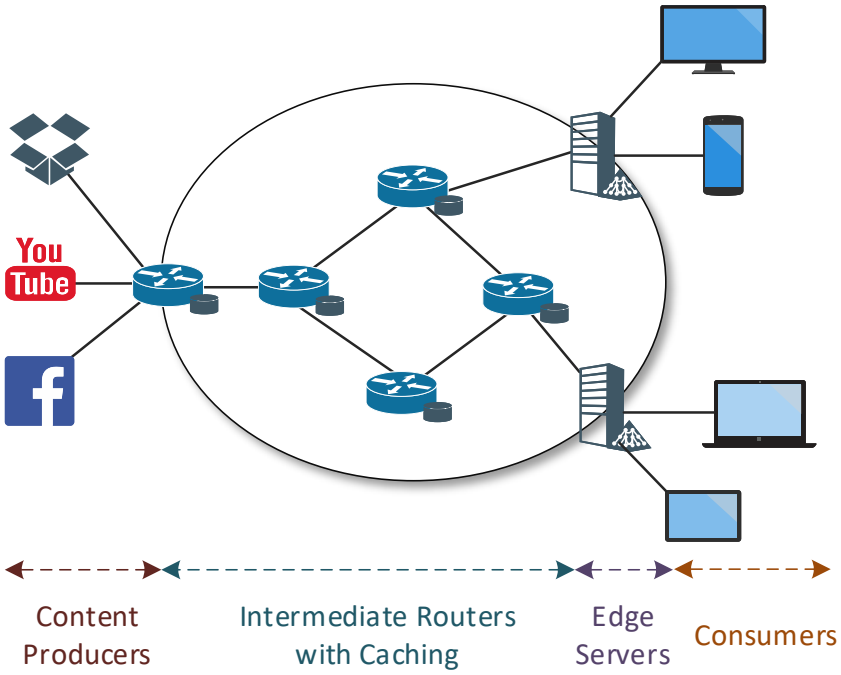
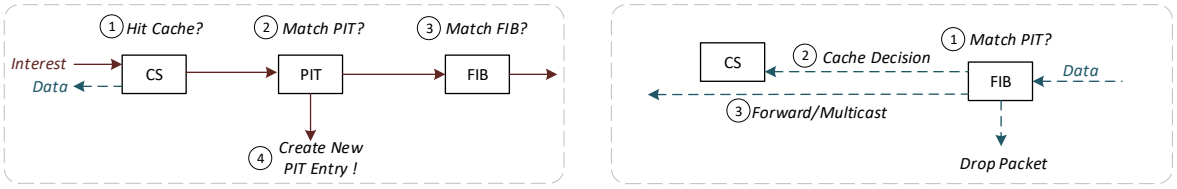


Fig. 3. Basic ICN communication model.

- *Hierarchical names* are made of a set of components to identify the application, describe the service or the content. The structure of a hierarchical name is similar to *Uniform Resource Identifiers* (URIs). Hierarchical names are usually user-friendly and convey semantic meaning to users. The hierarchical naming scheme enhances the network scalability since the name prefix can be aggregated and hence accelerate the lookup process.
- *Flat names* are generally produced by applying hash algorithms to content. Flat names have neither a semantic meaning nor a structure. Therefore, the name is not human-friendly and hardly assigned to dynamic contents that are generated by demands. Flat naming cannot support routing aggregation, hence their scalability is an open issue.
- *Attribute-Value based names* have a collection of attributes, in which each attribute has a name, a type, and a set of possible values (e.g., creation date, content type, version.). These attributes describe a single content piece along with its properties. Attribute-value based naming provides a mechanism for easy search operations through keywords. However, ensuring name uniqueness is challenging as one search request may lead to multiple results.
- *Hybrid names* combine at least two of the previous schemes. The overall idea is considering features provided by different schemes to improve network scalability and performance, and heighten security and privacy. For example, taking advantage of name aggregation to enhance lookup operations, the fixed length of flat names to improve memory consumption, and attribute values for keyword-based search operations.

2.1.2 Content-based Forwarding. By adopting name instead of host address to identify content, ICN uses name-based routing [10] to discover and deliver content to the requester. Due to the receiver-driven design, a consumer triggers a request for a specific content just by specifying its name. The request is forwarded hop-by-hop using a



(a) Data Discovery. (b) Data Delivery.

Fig. 4. NDN forwarding process.

forwarding/routing table and the requested content name to find a cached version of the content in the network or reach the original producer. When the content is found, the data delivery process takes place to send the content back to the requester.

2.1.3 In-network Caching. Due to the use of location-independent and self-contained data packets, ICN enables in-network content caching [26] during communication. The network becomes aware of content discovery and delivery [85, 128]. In the ICN-based network, each node has the potential to cache content at the local cache-store and satisfy future demands. Therefore, the network witnesses massive improvements in terms of communication delay, content retrieval process, and quality of service.

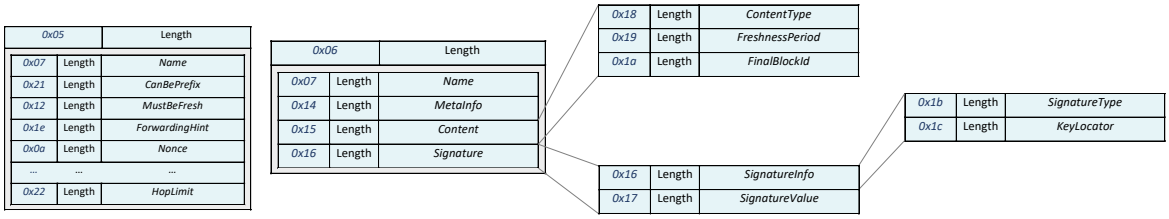
2.1.4 Content-based Security. Due to the use of naming abstraction and in-network content caching, ICN adopts content-based security [137], in which security-related mechanisms are applied to the content itself rather than the communication channel/session. Different trust models have been introduced based on network services [34, 51, 56, 115, 139]. Besides, each data packet in ICN can be authenticated, while security-related information is bound to the content (e.g., the publisher's public/secret keys and signature).

2.1.5 Mobility Support. From the ICN perspective [142], the content is decoupled from time and space. The content name is the only element used to discover and deliver it back to the consumer. When an ICN node moves from a network to another, it can re-issue any unsatisfied requests, and the producer or replica-node replies with the requested content without the need to request a new address during the movement. However, in this case we face two major issues: How the requested data can be delivered to a mobile consumer since no addresses are used, and how a consumer can request a data from a mobile producer? Another challenge arises in the case of producer mobility, specifically, how content can be retrieved from mobile producers [97, 123, 163].

2.2 Named Data Networking (NDN)

NDN [162] is the most prominent realization of the ICN vision [121]. NDN uses two types of packets: Interest and Data. Interest packets are triggered from a consumer, in the form of a request message to ask for content from the network. The provider node or any replica node can reply with a Data packet that carry the requested content toward the consumer [73]. Both Interest and Data packets carry the name of the requested content. NDN is a named-based network where the routing plane is done by using names instead of IP addresses. NDN implements hierarchical, human-readable, and structured names. Moreover, NDN maintains three data structures: Content Store (CS), Pending Interest Table (PIT) and Forwarding Information Base (FIB). Figure 4 illustrates the forwarding engine in Named-Data Network that can be divided in Data Discovery and Data Delivery:

Data Discovery: After receiving an interest packet, the forwarding node consults its local CS to check if a copy of the requested content exists. If a match is found in the CS, then a data packet is sent out via the same interface that the interest packet was received. Otherwise, a PIT lookup is performed to verify if the same interest



(a) Interest Packet. (b) Data Packet.

Fig. 5. Interest and Data packet structure.

has been already forwarded. If a PIT match is found, the node adds the received interface ID to the PIT entry (also referred to as interest aggregation) and discards the interest packet. Subsequently, the FIB table is consulted to find the most suitable interface to reach the requested content. If a match is found, a new PIT entry is created using the requested content name and the ID of the received interface, and the interest packet is forwarded upstream via one or more outgoing interface(s) according to FIB [21, 84].

Data Delivery: In contrast to the interest forwarding process, only the PIT is involved in data forwarding. When a node receives a data packet, it checks the PIT to verify whether the associated request has been already forwarded via the node that receives the interest packet. If no match is found in the PIT table, it means that no interest carrying this name has been forwarded and thus the data packet is considered unsolicited and is dropped. Otherwise, the node forwards the data to all listed interfaces in the PIT entry (multicast), and expunges the PIT entry. In the meantime (according to the current caching placement strategy), the data may or may not cached in the local CS.

2.3 NDN Applications

NDN is a receiver-driven architecture that can be integrated as a communication enabler for almost all kinds of today's applications and use cases [74]. Below, we discuss existing efforts on areas that can benefit from access control mechanisms, such as the Internet of Things, Vehicular Networks, peer-to-peer applications, and distributed dataset synchronization protocols.

2.3.1 Internet of Things. In the coming years, there will be billions of connected smart devices such as sensors, smartphones, cars and data centers, deployed in any environment with computation capability and interoperable interconnection, exchanging information online. These form of connection is known as the Internet of Things (IoT) [8] that will be deployed with sensing and intelligence capabilities so that they can not only communicate, but collecting data, negotiate, collaborate and exchange the collected values.

Deploying IoT applications of top of ICN [87, 88, 101, 102] is promising to enhance the overall network performances. Indeed, most of information produced by IoT smart devices can be regarded as content [108], consumers in the networks request data in IoT context without the need of the location of the sensors or the actuator, no end-to-end session is required for content retrieval [104], where ICN target the content in the network by its name rather than its address. Also, most of IoT devices request the same content in the network such as asking for humidity value for a specific place, or query some information, or data monitoring [103]. In the second hand, we find out that ICN nodes can act as node-replica by using content store, and serve for future requests regardless of the content reachability from the original source, that improve the data retrieval, and reduce the latency [55, 99, 105, 124]. In such scenarios, NDN is more suitable for IoT than IP, not only for the rapid content delivery, but also for its receiver-driven design, and request aggregation [59, 63, 87].

2.3.2 Vehicular Networks. Recently, substantial efforts and funding projects have been shown in the area of Vehicular Ad hoc Networks (VANETs) [91, 119]. The main purposes of vehicular networks and applications are to provide a comfortable life, efficient transportation & safety services, and secure data sharing. However, the characteristic of vehicular communication is more challenging especially with the high and dynamic movement of vehicles that affects the network topology and the reliability of communication [90, 95, 148].

Towards the merger of NDN with VANET networks [58], various research efforts have been proposed to enhance the core NDN architecture or target different features and aspects [7, 46, 57]. The use of content name to identify services and content may help to provide more independent communication, especially when mobility factor is taken into consideration [52, 53, 98]. Coupling the naming with in-network caching is also promising to improve the overall network performance and providing an efficient content delivery [60, 112]. A mobile node is not required to get a new IP address when move from a network to another. Indeed, it is only required to send a request packet specifying the required name. Doing so, the mobility issue can be enhanced.

2.3.3 Peer-to-Peer Applications. Peer-to-peer applications, such as BitTorrent for file sharing, have faced several challenges running on top of TCP/IP. Among others, such challenges include peer discovery, peer selection, and traffic localization [82, 83, 86]. In NDN, the content is decoupled from the location of its production and as a result, explicit peer discovery and selections mechanisms are not needed since the NDN forwarding plane will retrieve the requested data from the closest peer that can offer it. Moreover, in-network caching and Interest aggregation can effectively mitigate flash-crowd scenarios, a common problem with TCP/IP-based peer-to-peer file sharing applications. Such applications capitalize on data sharing, therefore, access control mechanisms may be useful to ensure that only authorized peers have access to certain pieces of data.

2.3.4 Distributed Dataset Synchronization Applications. NDN transforms the problem of synchronizing datasets in a distributed manner to a problem of namespace synchronization. Several synchronization protocols have been proposed both for infrastructure-based [25, 35, 36] and infrastructure-less environments [71]. In this use-case, access control mechanisms can be used to determine which entities can join a synchronization group and get access to the synchronized dataset.

3 COMMUNICATION SECURITY IN NDN

Indeed, the use of content names instead of host addresses allows the network layer to decouple the content from its original location, consequently enabling in-network caching. This feature promises to distribute the content towards different locations [81], usually close to consumers, in order to decrease the delay, improve the quality of service [54], and cover a large number of consumers regardless of the availability of the original content producer. In such cases, the original producer loses the control over its content including security, privacy, and access control [17, 109].

3.1 Content-based Security

Traditional security protocols [147] such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL) may not be a good fit for NDN as they are based on building a secure channel or session between the content producer and the consumer. However, in NDN, content may be delivered from different locations and content stores; some content can be delivered from the network edge nodes, while other may be satisfied by neighboring nodes or intermediate nodes at the core network (i.e., ISP – Internet Service Provider) [13, 20, 141].

Content-based security concept tends to provide the main security and privacy services [12] such as:

- *Confidentiality*: Confidentiality refers to the task of protecting the content from being accessed by unauthorized users. Only the users who are authorized to do so can gain access to sensitive data. If the system fails to maintain confidentiality, a user who should not have access has the ability to get it.

- *Integrity*: Integrity refers to the task of ensuring the authenticity of content (i.e., the content itself or the producer of the content have not been forged). If the system fails to provide integrity, anyone in the network can provide content and pretend that they re the owners of the information.
- *Authentication*: Authentication refers to the process of ensuring and confirming a user's identity. If the system fails to provide authentication, anyone in the network can access any content regardless of their identity or credentials.
- Availability: Availability refers to the task of ensuring that authorized parties are able to access the content when needed.

The content-based security concept aims to secure the content itself on a per packet basis rather than securing the communication channel [76]. Fundamentally, NDN packets are encoded using a Type-Length-Value (TLV) format [3]. Figure 5 illustrates both Interest and Data packet encoding. Each packet is a collection of TLVs, where a TLV may contain nested TLVs. NDN forwarders identify these packets using their type, while each TLV has a unique type.

In NDN, each Data packet is secured and cryptographically signed [120, 157]. The TLV `Signature` specifies all information related to the packet signature including: (a) `SignatureInfo`: to describe the signing algorithm, and relevant information about certificates and keys; and (b) `SignatureValue`: to represent the signature itself in bits. It is important to highlight that regular Interest packets are typically not signed; however, NDN introduces *Interest Signature* to produce signed Interest packets. NDN supports a wide range of signatures such as *DigestSha256*: using SHA-256 digest for data integrity that produces only 32 bytes; *SignatureSha256WithRsa*: using an RSA signature over a SHA-256 digest which is an efficient asymmetric encryption method where we only need to verify that the data has not been tampered; *SignatureSha256WithEcdsa*: using an ECDSA signature over a SHA-256 digest, however ECDSA signatures are not deterministic and they depend on a random number generator to generate the signatures that may have a different value after each signing operation, hence the correctness of the value of these signatures can only be tested by verifying with the public key; and *SignatureHmacWithSha256*: using a SHA256 hash-based message authentication codes. The efficiency and performance of these signature algorithms vary and are mainly based on the used encryption algorithm.

Content retrieval in NDN shifts from the session-based security towards content-based security. It aims to provide different security and privacy services. In the next section, we discuss what kind of cryptographic algorithms, security protocols, and techniques can be used to provide the core network security.

3.2 Cryptographic Algorithms & Security Protocols in NDN

Most existing cryptographic algorithms and security protocols can be applied to NDN with slight or more extended modifications. This section provides a comprehensive overview of such algorithms and protocols, Table 2 summarizes our discussion.

3.2.1 Hash-based Signatures. Hash-based signatures [19] ensure the integrity and authentication of NDN data packets. Various hash-based signing algorithms can be used in NDN such as RSA and ECDSA, which are characterized by high and fast signature generation and verification with private and public keys. Moreover, these signatures are usually based on an One-Time Signature (OTS) system [126] that allows the use of key pairs to only sign one message securely. An N-time signature system is another way that allows signing N messages securely. The Merkle Signature Scheme (MSS) [18] is another hash-based, N-time signature system that uses an OTS system as an element. MSS is a binary tree that has a height h that is used to create 2^h OTS key pairs. Each node in the tree has a value that represents the hash values of its child nodes. The public key is the value of the root node, while the private key is the combination of all OTS private keys with the index of the next OTS private key.

Table 2. Cryptographic algorithms & security protocols in NDN.

Approach	Features	Target	Level	Storage	Computation	Drawbacks
Hash-based Signatures	• Ensure integrity and authentication • RSA, ECDSA, and MSS • High and fast signature generation • Small-sized private and public keys	• Integrity • Authentication	C, P	H	M	• One-time signatures • Signature size
DPI	• Ensure content privacy • Inspect packets • DPI, Blind-Box	• Integrity	R	M	H	• Violate name and user privacy • Select trusted router(s)
Key Exchange	• Allow the use of cryptographic algorithms • Session-based communication • Diffie-Hellman	• Integrity • Authentication	C, P	H	M	• One-to-many communication • Many-to-many communication
PIR	• Prevent the host from identifying requested content.	• Integrity	R	L	H	• Design and implementation complexity

** C: Consumer, P: Producer, R:Router | L: Low, M: Medium, H: High*

3.2.2 Encrypted Deep Packet Inspection. Deep Packet Inspection (DPI) [154] can be used in NDN to inspect packets and check whether they contain sensitive data. This process violates content and user privacy. However, by encrypting the packet payloads, DPI cannot be performed, and the privacy services can be preserved. Blind-Box [129] has been proposed in order to perform the DPI directly on encrypted payload. It is based on two main classes of DPI computation with different privacy assumptions and guarantees: exact match privacy and probable cause privacy. The first class includes DPI applications that depend on exact string matching, while the second class can support all DPI applications. NDN uses plaintext names instead of IP addresses, which raises concerns over content privacy. Using encrypted or pseudo names may alleviate such concerns, but still, name obfuscation may interfere with name-based routing. Finally, how to select a trusted anonymizer for name obfuscation is an open question.

3.2.3 Key Exchange. Key exchange, also known as key establishment, is an important security aspect of asymmetric crypto-systems, so that keys between communicating parties are exchanged in order to be used in cryptographic algorithms. Diffie-Hellman [78] is probably the most widely-used key exchange protocol. This algorithm assumes session-based (point-to-point) communication, thus requiring modifications for communication among multiple parties (one-to-many or many-to-many communication) [25, 71, 72]. Hence, a secure group-based protocol is more suitable for such scenarios [110]. The content producer may generate a new key pair (public/private keys) based on the number of active subscribers in the communication to secure the published content. It is important to highlight that the key exchange/generation protocol should be aware of the active subscribers, previous active subscribers should not be allowed to decrypt newly generated content. Also, whenever a new subscriber joins/leaves the subscription, the protocol should exchange/generate new key pairs [14].

3.2.4 Private Information Retrieval. Private Information Retrieval (PIR) is a cryptographic primitive widely used in databases. It aims to prevent the database server or the host service from identifying which record has been requested. This concept is important in ICN/NDN. Related work has investigated private lookup operations for named data [138], essentially hiding information about the names of the data packets that were retrieved.

Table 3. Summary of access control mechanisms.

Approach	Features	Level	NDN Applicable	Storage	Computation	Drawbacks
Identity-based Encryption	• Generates public keys from known unique identifiers • Does not require distribution public keys	C, P	✗	M	L	• Third party authentication • Requires a centralized server • Requires a secure channel
Attribute-based Encryption	• Uses a set of attributes • Provides fine-grained access control	C, P	✓	L	L	• Challenge of attribute revocation
Role-based Authentication	• Use of the role concept • One-to-many communication model • Key revocation	P	✗	H	H	• Additional overhead • Not suitable for dynamic network conditions • Third party authentication
Key-Policy-based Authentication	• Provides fine-grained access control • Determines which attributes to use with content	C, P	✓	H	H	• Additional overhead • Third party authentication
Multi-Authority Authentication	• Uses attributes from different authorities • Uses symmetric encryption • Expressive and efficient scheme	C, P	✗	H	H	• Additional overhead

** C: Consumer, P: Producer | L: Low, M: Medium, H: High*

3.3 Access Control Mechanisms

Authentication and access control are important security aspects, especially with the increase in the devices that generate content. To this end, various access control solutions have been proposed in the literature. We further discuss these concepts including their pros and cons below. Table 3 summarizes this discussion.

3.3.1 Identity-based Encryption. Identity-based encryption is an AC technique based on public key infrastructure. A private key generator is used to generate master public and private keys. A user is able to decrypt the content by getting the master private key after getting authenticated by the private key generator through the user identity. This scheme aims at reducing the complexity of the encryption process, however the whole system is based on trusting the third party that generates the master keys and authenticates users.

3.3.2 Attribute-based Encryption. In Attribute-based Encryption, an attribute authority generates public and master private keys for a content producer. The content owner uses a set of attributes to allow authorized users to access content as well as generates the keys subsequently used to encrypt content. A content consumer uses his/her own private key to decrypt the content if the attributes are matched. Although this scheme provides fine-grained access control, the attribute authority needs to use the public key of each authorized user to generate keys and encrypt content.

3.3.3 Role-based Authentication. In role-based authentication, the content owner uses the role concept to authenticate users and encrypt the content. A role is assigned based on the responsibilities and qualifications of an entity. An authenticated user has the privileges to access content according to the assigned role. A third-party entity or the content owner can manage the responsibility to assign roles, and consequently revoke a role if a user is no longer authorized. This scheme is suitable for one-to-many communication model and easy to implement

and handle key revocation; however, it may result in overhead in cases of dynamic changes of the users joining and leaving the communication group.

3.3.4 Key-Policy-based Authentication. In key-policy-based authentication, the encrypted content is attached with a set of attributes. The private key issued by a third party is associated with an access policy structure that describes the user's identity. A user can decrypt content only if the access policy in his private key satisfies the attributes attached with the encrypted content. Although this scheme may provide fine-grained access control, deciding which attributes to use, attaching them to the content and using an extra access control structure produce overhead and may not scale well.

3.3.5 Multi-Authority Authentication. Multiple authorities issue attributes to users and assign an access policy structure to the content using attributes from different authorities. The content owner divides the content into different chunks in which each chunk is encrypted using symmetric encryption techniques, defines a set of access policies using attributes from multiple attribute authorities, and then encrypts the content. A user can decrypt the content only if his/her attributes satisfy the access policy associated with the content. However, managing the various authorities and attributes may result in considerable overhead.

The aforementioned schemes are widely used in today's IP-based networks. Migrating them to content-oriented networks require modifications especially due to the use of ubiquitous in-network caching and content naming. In the following sections, we review the existing NDN-based AC solutions. We broadly classify them into two main categories: encryption-based and encryption-independent AC solutions.

3.4 Insights & Learned Lessons

NDN provides numerous advantages over the IP-based Internet such as efficient data dissemination, in-network caching, and content-based security. In fact, content-level security is promising to enforce security at the content itself rather than the communication channel. Authentication and access control rules can be applied to the content and not the provider. Hence, all rules and access policies need to be associated with the content during transmission and caching.

Some of the key learned lessons that should be noted are the following:

- In ICN/NDN, naming becomes a '*shared*' layer between applications and the network. To this end, ICN transforms the problem of designing access control mechanisms to the design of appropriate naming schemes that determine the permissions of each entity for access to produced content. Naming also facilitates the realization of attributed-based access control mechanisms.
- ICN/NDN offers built-in security mechanisms directly at the network layer. Such mechanisms, apart from securing the retrieved content itself, can be used to secure the retrieval of access control rules, certificates, and encryption/decryption keys.

4 ENCRYPTION-BASED ACCESS CONTROL

In this section, we review existing encryption-based access control solutions in NDN. We refer to an encryption-based scheme as the process where the content producer encrypts the content and establishes access control rules. The content consumers must explicitly get authenticated by the publisher. The existing solutions have been further classified into subcategories based on the types of encryption. Table 4 summarizes the reviewed solutions.

4.1 Attribute-based Access Control

Attribute-Based Encryption (ABE) [41] incorporates public-key encryption where the secret key heavily depends on a set of attributes. Here, we differentiate two main types of ABE: (a) Key-Policy Attribute-Based Encryption (KP-ABE) [69]: the access tree is represented by a set of secret keys that define the privileged scope, and (b)

Table 4. Summary of Encryption-based access control mechanisms.

Ref.	Approach	Level	Content	Cache	O/H	Comp.	Major Drawbacks
			Attribute-based Access Control				
[47]	• Attribute based encryption mechanism	C	Dynamic	✓	H	L	• No evaluation presented • Missing revocation schemes
[68]	• Privacy preserving for published and cached content	C, P	One-Time Usage Content	✓	L	L	• Relies on a trusted third party
[24]	• Attribute based encryption with revoked privileges	N	Dynamic	✓	H	M	• Third party authentication • Single point of failure • Proxy needs to be always online
[67]	• Attribute-based encryption naming scheme	R	Dynamic	✓	H	H	• Feasible only with flat names • Cannot be applied to hierarchical names
[42]	• Access control management based on attribute encryption	N	Static	✓	H	H	• Third party authentication • Component placement and communicate models are missing
[15]	• Use of central authority for attribute-based Encryption	N	Dynamic	✓	L	H	• Use smaller policies • Authority problem
[152]	• Ciphertext policy using attribute encryption.	P	Static	✓	H	L	• Requires publisher to be always online.
[153]	• Use of attribute authorization entity.	C, P	Static	✓	H	H	• Relies on proxy security
[117]	• Use of attribute-based signatures.	C, P	Static	✗	H	H	• Costly verification process • Large signature size
			Name-based Access Control				
[45]	Identity-based cryptography mechanism	P	Dynamic	✓	H	M	• Clients can access previously published content • Does not scale well
[150]	• Session-based mechanism	P	Dynamic	✗	H	H	• Replicated content in the network
[44]	• Data-based access control using encryption and lock password	P	Static	✓	M	H	• Hard to generate/update access rules
			Identity-based Access Control				
[151]	• Combining proxy re-encryption with identity-based cryptography	C, P	Static	✗	M	M	• Requires publisher to be always online
[31]	• Use of rendezvous points to enforce AC in pub-sub	P	Static	✗	H	H	• Heavy and intensive computation • Requires publisher to be always online
[43]	• Access control using certified credentials	P	Static	✗	M	M	• Use of a centralized entity • Not efficient in large-scale networks
[140]	• Fine-grained access control.	C, P	Static	✗	H	H	• Trust-ability issues
			Re-encryption-based Access Control				
[79]	Update of access rules at content stores	P, R	Static	✓	H	H	• No guarantees in terms of updating all cached versions • Necessitates the availability of original producer
[166]	• Dual-phase encryption mechanism • One-time decryption key, proxy re-encryption, all-or-nothing transformation	P, R	Static	✓	H	H	• Scalability is an open question • Necessitates the availability of original producer • Trustability of edge routers
			Broadcast-based Access Control				
[93]	• Broadcast decryption keys in the network	P, C	Static	✗	H	H	• Large number of broadcast keys
[94]	• Broadcast secure content at CS	P, R	Static	✗	H	H	• Dynamic changes of in-network content stores
			Probabilistic-based Access Control				
[22]	• Probabilistic encryption to prevent unauthorized access	P	Static	✗	H	H	• Requires publisher to be always online • Impact of false positive errors

** N: Network C: Consumer, P: Producer, R: Router | L: Low, M: Medium, H: High*

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [50]: the access tree is represented by attributes in a ciphertext. The main advantages of ABE is that it is flexible and may provide access control enforcement to a group of users [11]. However, it must be deployed based on a single and centralized authority, a fact that may affect the scalability of the system.

Ion *et al.* [47] propose an attribute-based encryption mechanism for content-centric data privacy in ICN by attaching the access control policies to the content itselfThe client decrypts the content only if its symmetric key

satisfies the access control policies that are included in the cipher-text or the key itself. However, the authors did not evaluate their solution in comparison with other proposed solutions.

Li *et al.* [68] introduce a privacy-preserving content access control scheme for content already published and cached by other nodes. The proposed scheme is based on Attribute-Based Encryption and requires a trusted third party with the responsibility to assign attributes to other entities. Any node in the network has a unique identifier and a set of attributes. The content producer assigns a combination of attributes to the content before its publication to specify who can access it without explicitly knowing the consumer. It also generates a random symmetric key to encrypt the content. The consumer uses its attributes to access the content, if the attributes satisfy the encryption policy, the consumer then gets the random symmetric key, and consequently decrypt the content. The major limitation of this system is that it is based on a trusted third party.

Da *et al.* [24] design an attribute-based encryption scheme to provide fine-grained access policies in NDN with the ability to revoke privileges. A proxy node is used to provide access to secured data and inspect rules for revocation. Consumers register in the network based on a set of descriptive attributes that allow the proxy to authenticate users [135]. The authors divide the content into two main parts: the content/data itself, and the structure to define access rules. The former can be cached by intermediate nodes, while the latter is cached and used only by the proxy node. Although this scheme may eliminate the necessity to connect with the original producer to fetch access rules, it allows proxy nodes to decrypt the content without any trust enforcement policies.

Li *et al.* [67] address the access control policies for distributed cached content in ICN. The authors propose an Attribute-Based Encryption naming scheme to tackle the management of content attributes in a distributed manner through an ontology-based management system and to enforce the access rules on public/cache-able routers through a set of name attributes. The main drawback of this scheme is that it is feasible only with flat naming schemes and cannot be used with hierarchical naming schemes. Similarly, Grewe *et al.* [42] introduce an attribute-based encryption access control scheme for vehicular networks. The authors define two main components: (a) an access control management component to manage different policies and access rules based on their attributes, and (b) a cryptographic component to encrypt content based on the policies defined by the access rules. However, the placement of these components (centralized or distributed) and how they communicate/exchange attributes and policies remain an open question.

Feng *et al.* [30] present a decentralized ciphertext-policy, attribute-based encryption mechanism to solve the revocation problem and preserve the consumers' privacy. In this work, the publisher creates an access control policy and encrypts the data according to this policy, current time, and the time that the data will be cached by routers. Then, it sends this policy in ciphertext in the network and hides the attribute values. Whereas, consumers can decrypt the ciphertext only if their attributes match the access structure in the ciphertext. The main drawback of this scheme is that the publisher needs to be always available. Similary, Wu *et al.* [152] propose a ciphertext policy, attribute-based encryption access control mechanism. In this scheme, the publisher splits the data into two sections: (i) the Public Content Section (PCS) that is the content itself, and (ii) the Content Key Section (CKS) that is a part of the key and specifies the data consumers. Consumers can decrypt the content by combining the PCS and the CKS. In doing so, they need to issue two interest packets, the first packet to request the PCS from the publisher or intermediate routers' content stores, while the second one to seek the CKS from the publisher. The main drawback of this work is that it requires the publisher to be constantly available which might not always be the case. Another proxy-assisted access control scheme is proposed by Wu *et al.* [153] to ensure forward and backward security and achieve the user and attribute revocation. This mechanism includes an attribute authorization centre that is capable of creating an attribute of public keys. The publisher generates the access control policy for attributes and encrypts the content which is disseminated in the network and cached by NDN routers. Consumers can get the encrypted content from routers or publisher by inquiring keys from the central authorization center, and get the partially decrypted content from NDN routers that is decrypted using the proxy

key. Consumers can then decrypt the remaining part to obtain the plaintext data. The main drawback of this work is that the increase in the number of attributes highly increases the proxy decryption time and ciphertext re-encryption.

Ramani *et al.* [117] introduce an alternative NDN signature design using attribute-based signatures to retrieve certificates and preserve the anonymity of individual publishers. In this approach, the publisher generates a policy by combining all attributes, then it creates a signature and adds it to the data packet. The consumer can verify the data based on two pieces of information: the data itself and the public key. The main limitation of this approach is that the verification process results in high cost, while the number of attributes increases the signature size. In [15], Borgh *et al.* extend Attribute-Based Encryption (ABE) for an IoT-based ICN architecture. Authors discussed two potential solutions. The first one is an ABE solution performed through a central authority. Sensors in this design encrypt the content through symmetric keys (encrypted by the central authority), which is then published through the ICN network. Users can access the content by decrypting both the symmetric keys and the content. The second solution is an ABE sensor system. In this solution, the central authority is not needed for encryption, since sensors perform ABE operations. The main drawback of these solutions is that they both use small-sized policies since sensors have limited computing resources.

4.2 Name-based Access Control

A Name-based Access Control (NAC) mechanism [164] provides an automated key management process and content confidentiality using an encryption algorithm based only on the content name. Hamdane *et al.* [45] propose an enhancement-based access control scheme by eliminating the use of access control lists and uses a new cryptographic model. The content is encrypted by namespace keys, which are available to all nodes under the same namespace. However, the proposed scheme did not account for dynamic changes and large scale networks. Wang *et al.* [150] designed a session-based access control solution for ICN. This solution uses two different names for each piece of content, public and secure names. Secure names can be identified only only by authorized users. The authors demonstrate their solution through the example of an Online Social Network (OSN), where each user communicates with OSN over a session, and he/she is associated with a unique key shared with the service. The content uploading process requires the user to be authorized by the OSN using the shared key. Therefore, a user receives content over a session as well as the symmetric key and the required metadata to decrypt the content. All this information is encrypted by the session key. The main drawback of this mechanism is the overhead associated with several replicas of content that may be available across the network.

Hamdane *et al.* [44] propose a data-based access control mechanism based on using encryption and lock password. In this approach, the access rights are established by the namespaces concept and specified in the access control list. This approach also provides a revocation mechanism by creating and encrypting a random key with public keys. The access control list is updated, and the revocation time is saved with the old password by the trusted server. However, creating and generating all the networks to add new access rights may become a challenging task.

4.3 Identity-based Access Control

In identity-based access control, the content consumer may prove its identity before requesting/consuming the content. The content publisher in return authenticates the requester before providing the content. Public or derivable keys are used to identify the consumers at the publisher level. Wood *et al.* [151] introduce a secure content distribution architecture on top of content-centric networks. This architecture is based on an identity-based cryptography and proxy re-encryption to provide simple public keys. These keys can be associated with users and pre-defined access rules. Although this mechanism may provide secure end-to-end communication, it requires the producer to be always connected, otherwise, consumers will not be able to decrypt the content.

Fotiou *et al.* [31] design an access control mechanism for publish-subscribe based on enforcing the access control policies by Rendezvous Points (RVs). A content owner creates an access control policy that is assigned and protected with an ID. This ID is used as a public key to protect RVs. The owner encrypts the content through a symmetric encryption key, which is then encrypted and decrypted through the IBE encryption algorithm and the ID. Hence, the owner stores encrypted contents, the encrypted keys, the decrypted keys, and the list of authorized subscriber identities. When a publisher receives content, it advertises content information to RVs. If a subscriber needs to get the content, it sends a subscription message to the RV to initiates an authentication process. If the subscriber identity is included in the list of authorized identities, the RV sends a notification to the publisher in order to deliver the content to the subscriber. The main drawback of this solution is that it incurs compute-intensive operations due to the IBE algorithm, which cannot be used in constrained devices such as IoT. Hamdane *et al.* [43] proposed a credential-based access control scheme for NDN. The proposed scheme assigns access rights to consumers based on certified credentials provided by an Access Control Manager (ACM), which is an entity that handles the private key(s) associated with the network namespace and defines the access and management rules. The communication and all security related operations are based on this centralized entity raising scalability concerns in the case of large-scale networks. Moreover, the proposed system requires an ACM for each namespace, the communication between ACMs in the case of different namespaces is an open question. Similarly, Tseng *et al.* [140] introduce a fine-grained access control mechanism for NDN based on four roles: Key Generation Center, Content Producer, Online Shop, and Customers. The Key Generation Center is responsible for generating secret keys for the users and the Content Producer is able to disseminate the encrypted content in the network. The Online Shop allows customers to access the content. It is worth mentioning that the selection of trusted Online Shops maybe a challenging task.

4.4 Re-encryption-based Access Control

A re-encryption scheme [133] may use two or more encryption operations to provide authentication or update the access rules [132]. Mangili *et al.* [79] design an encryption-based extension for ICN. The proposed scheme aims to: (a) enforce confidential data dissemination: the producer encrypts the content, while the intermediate nodes cache encrypted rather than plaintext content; (b) track content access: consumers are authenticated by the original producer and fetch the required decryption keys; and (c) support policy evolution: producers may update the access policy through key-derivation and re-encryption. Although the proposed scheme is able to update the access policies after publishing the content, there is no guarantee to update all cached content instances. Also, the system is based on the availability of the original producer to retrieve keys for content decryption. Zheng *et al.* [166] introduced a dual-phase encryption mechanism that combines an one-time decryption key, proxy re-encryption, and all-or-nothing transformation. The original producer encrypts the original content with a key derived from its private key. When a consumer sends a request for specific content, the associated edge router re-encrypts the content (which is already encrypted by the producer) with a random key (each content has a different random key). The consumer is required to use both keys from the original producer and edge router to decrypt the content. Hence, the producer may control who can access the content. This scheme requires two keys for encryption/decryption, this the scalability is an open question. Moreover, the system is based on the availability of the original producer and the trustability of edge routers.

4.5 Broadcast-based Access Control

A broadcast-based access control tends to provide distributed access control to a group of users. The publisher encrypts the content and broadcasts the access rules to the network where only legitimate consumers may decrypt it. Misra *et al.* [93] introduce a broadcast-based access control solution to secure content delivery in ICN. The content is encrypted by the producer using a public key, then the producer broadcasts this key into the

network. The client can decrypt the content only if its symmetric key is matched with the public key. The main drawback of this scheme is that the number of keys broadcast in the network may be large severely affecting the network bandwidth. Misra *et al.* [94] tackled the limitation of requiring access control rules to be retrieved only from the provider. Hence, they propose an access control framework that allows a legitimate user to access and consume content directly from in-network caches without the need to be authenticated directly by the producer. The authors designed a broadcast encryption mechanism; the original producer broadcasts content to a set of legitimate consumers in a secure manner. However, a change in legitimate consumers (e.g, revoking the access privileges of a consumer, adding new consumers) is an open issue and requires further investigation.

4.5.1 Probabilistic-based Access Control. A probabilistic-based access control scheme integrates a probability function to determine if a request is authorized to access the content. Chen *et al.* [22] proposed a probabilistic encryption-based access control mechanism for video streaming services over NDN. The proposed mechanism supports symmetric/asymmetric cryptographic operations to encrypt video content. The authors used Bloom filters to store the public keys of authorized consumers in order to filter invalid requests. The main drawbacks of this mechanism are the need for an always online producer and the impact of Bloom filter false positive errors.

4.6 Insights & Learned Lessons

One of the promising features of NDN is decoupling the content from its production location, which leads to in-network caching. The use of encryption-based access control mechanisms requires that all access rules need to be executed/enforced at the original producer level. This type of solution necessitates the original producer to remain connected and reachable at all times.

Some of the key lessons learned that should be noted are the following:

- Dynamic content is widely used on the Internet. Access control schemes should be able to generate policies and rules upon the creation of the content with minimal overhead.
- Decoupling access control rules from content may help to identify unauthorized consumers, however, this solution violates ICN primitives, where the security-related information should travel with the content and be cached with it.

5 ENCRYPTION INDEPENDENT ACCESS CONTROL

In this section, we review existing encryption independent access control solutions. We refer to an access control solution as encryption independent if the access rules are determined independently from any underlying encryption. Existing solutions have been further classified into subcategories based on how rules are defined. Table 5 summarizes the reviewed solutions.

5.1 Broker-based Access Control

In broker-based access control, a third party entity is used as a broker for the communication to apply and verify access control rules. The security of the whole system is based on the trust of this third party entity. Fotiou *et al.* [32] introduced an access control mechanism for ICN to protect the information of consumers and preserve their privacy. The proposed mechanism secures the information of consumers based on access control policies that are created by an Access Control Provider (ACP), who interacts with publishers, Rendezvous Nodes (RNs), and subscribers. Each publisher sends its access control policy to the ACP to have a URI assigned to it and then forwards the content to the RN. The RN sends the policy URI to the subscribers that request the content and, at the same time, the RN sends the URI of the associated policy to the ACP. Subsequently, the ACP verifies the policy and notifies the RN if the subscriber is allowed to access the content. If the verification is successful, the RN forwards the content to the subscriber. This mechanism produces additional computation and communication overhead at RNs that may increase the response latency. It also raises scalability concerns as the scale of the

Table 5. Summary of Encryption Independent access control mechanisms.

Ref.	Approach	Level	Content	Cache	O/H	Comp.	Major Drawbacks
			Broker-based Access Control				
[32]	• Use of AC Provider to coordinate access rules	N	Static	✗	H	H	• System security relies on the AC Provider • Requires extra overhead that may affect network delay
[131]	• Use of broker to store different access policies	N	Static	✗	H	H	• System security relies on the broker • Requires identification/verification of subscribers/publishers
[167]	• Lightweight time-based access control.	N	Static	✗	H	H	• Scalability issues with mobility
[155]	• Edge-based access control framework	N	Static	✓	L	L	• Performance based on edge node
			In-network Cache Enforcement Access Control				
[136]	• Enforces copyright when retrieving cached content	P, R	Static	✗	H	H	• Caching of split content is not feasible in real scenarios • Necessitates the availability of original producer
[64]	• Bypass censorship using consumer-driven access control	P, R	Static	✗	H	H	• Solution is not feasible in off-path mode
[80]	• Content-attendant policies in named function networks	C, P	Static	✗	H	H	• Extra communication overhead to identify consumers • Necessitates the availability of original producer
[75]	• Collaborative data access control scheme	C, P	Static	✓	H	H	• Overhead the network
[77]	• Blockchain matching-based access control	P	Static	✓	H	H	• Requires publisher to be always online
			Manifest-based Access Control				
[65]	• Decouples content and access rules using a manifest file	P, R	Static	✗	H	M	• Access rules are not cached with content • Necessitates the availability of original producer
			Interest-based Access Control				
[38]	• Use of interest packets to enforce access rules	C, P	Static	✗	H	M	• Requires mutual trust between consumer and provider • Identical content with multiple names remains an open issue
			Signature-based Access Control				
[70]	• Lightweight integrity verification	P, R	Static	✓	M	L	• Token refresh mechanism is required

** N: Network C: Consumer, P: Producer, R: Router | L: Low, M: Medium, H: High*

network grows. Singh *et al.* [131] presented an access control approach for pub/sub networks. This approach secures the information based on access control policies specified by a local broker, who is an entity that verifies consumers and producers, as well as manages the constraints and the associated access levels. Both consumers and producers need to register with their local broker and define their credentials and attributes before starting the communication. This approach results in considerable overhead, while the access level identification/verification and the creation and management of the network between producers and the broker was not discussed.

Zhu *et al.* [167] design a lightweight, time-based content access control mechanism based on the notion of content subscription times. This approach is based on three cryptographic techniques: proxy re-encryption, identity-based encryption, and broadcast method, which allow the provider to encrypt their content, and push it to distribution servers. Then distribution servers re-encrypt, broadcast, and distribute this content to the network. In this approach, consumers can decrypt the content based on the private key and the specified subscription-time. However, this approach did not consider mobility and scalability. On the other hand, Xue *et al.* [155] propose an edge-based access control framework for ICN to push the access control at the network edge and block unauthorized requests. The authors also propose a lightweight, privacy-preserving authentication protocol for the communication between consumers and edge routers based on group signature and hash chain techniques. This approach provides a revocation method, but results in considerable overhead without considering access control among different providers.

5.2 Cache Enforcement-based Access Control

In-network caching is a building blocks of NDN that improves the overall network performance. Both content caching and cache hits occur in a transparent way without informing the original producer or requester. The producer loses control over who can cache the content, which results in privacy, ownership, and copyright issues. Cache enforcement access control schemes aim to address this issue. Tan *et al.* [136] tackled the uncontrolled in-network caching problem for copyright enforcement during content retrieval from content stores. Authors argue that solutions based on encryption cannot protect content copyrights during caching. Hence, they proposed splitting large sized content into two parts: a big part and a small part with the constraint that without the small part no one can rebuild the whole content. The authors suggest that any node in the network can cache the big part of the content, while the small part remains at the original producer. To rebuild the content, the authors use bit-wise OR operations. The main drawback of this scheme is that the producer must be continuously connected to control the access policies. Kurihara *et al.* [64] designed an anonymization system to bypass censorship in content-centric networks. The authors designed a consumer-driven access control scheme that incorporates encryption-based access control into interest names and allows the producer to recycle specific content cached at intermediate content stores along the communication path. Plain-text routable names are used in the initial phase of communication, while encrypted names are used to provide anonymous communication. The main drawback of the proposed system is that it targets only on-path intermediate nodes, while cached content off the communication path cannot be recycled.

Marxer *et al.* [80] presented a set of content-attendant policies to complement content-based security principles in Named Function Networking (NFN) computations. In this approach, each content piece has an Access Control List (ACL) that contains the list of consumer identities that are permitted to access the content. Consumers send interests that have their public keys (identities) attached. When a provider receives such interests and determines that a consumer's public key matches a key in the ACL, the provider sends back the requested content (symmetrically encrypted) along with a symmetric key (asymmetrically encrypted with the consumer's public key). When the consumer receives the symmetric key and the content, it first decrypts the symmetric key and then uses this key to decrypt and access the content. A consumer can also request and retrieve the ACL of a content piece. In this way, the consumer can become an independent content provider after receiving the content, ACL, and symmetric key. This approach, however, did not address the exchange of encrypted information in highly dynamic networks, such as vehicular networks.

Liu *et al.* [75] design a collaborative data access control scheme for NDN, where access control function is carried out at routers that may cache content instead of a single content producer. In this approach, the producer encrypts the content using a symmetric key. It then disseminates the key along with a unique sub-key for this content to the routers. When a consumer needs to access the content, it sends an Interest packet to request the encrypted content from the producer or a router. After that, the consumer sends another Interest packet to the cache-enabled router requesting the sub-key in order to decrypt the content. However, the authors did not discuss the generation of sub-keys, while their solution requires additional Interest packets in order to retrieve the content and the encryption keys. In another work, Lyu *et al.* [77] propose a matching-based access control model based on Blockchain to ensure the security of sharing, auditing, and revocation of the content's publisher. In this work, the publisher defines the permitting operations for each content, classifies the requesting nodes based on their attributes, and identifies the access right of the requesting nodes. This access right is transferred in the form of transactions on the Blockchain to ensure the security of transmission and accurate record keeping of access activities. This approach also allows routers to cache content in ICN only if the share operation is included in the permitting operations, and any requester can decrypt the shareable content by using the transaction of access taken for shareable content. However, the publisher needs to be always available to provide the operations for requesters and content.

5.3 Manifest-based Access Control

Manifest-based Access Control aims at providing a separate file (manifest) that specifies the access policy and rules, thus decoupling the access control rules from the original content. The main objective of this type of access control is to ensure minimum communication overhead and maximum utilization of in-network caches. Kuriharay *et al.* [65] proposed an encryption-based access control mechanism for content-centric networks. This scheme is designed from the perspective of manifest-based control retrieval. The idea consists of securing the content manifests and decoupling the encrypted content from access rules. To retrieve a content piece, a consumer needs to get authorized by the original content producer and download an encrypted content copy. Then, the consumer will use the manifest file to locate the required keys to decrypt the content. The main drawback of this scheme is that both the original producer and a consumer need to be simultaneously connected. This contrasts the design principles of ICN/NDN, where communication shall be session-less, the content is decoupled from the location it was originally produced, and the content consumption may be asynchronous compared to its production.

5.4 Interest-based Access Control

Interest-based Access Control mechanisms consist of attaching information to interest packets, which is used to determine the access rules for the requested content. Therefore, access control can be enforced even for cached content. Ghali *et al.* [38] designed an interest-based access control scheme to enforce access rules through the use of information in interest packets. In this scheme, access control rules and content-encryption are decoupled; the original content producer has the ability to enforce any access control rules without dealing with content encryption or key distribution. This scheme also supports both hash- and encryption-based name obfuscation, so that sensitive content names cannot be predicted by unauthorized entities. Moreover, mutual trust verification between routers and consumers was proposed to authorize access to locally cached content and overcome interest replay attacks. Despite the advantages of using obfuscated content names, the same content may be cached multiple times under different names, which can negatively impact the distribution of cache resources.

5.5 Signature-based Access Control

Signature-based Access Control mechanisms consist of a universal content signature verification process to enforce access control rules. Li *et al.* [70] extended the NDN architecture and proposed a lightweight integrity verification architecture. The proposed architecture uses one-way hash functions based on the Merkle Hash Tree algorithm to produce content signatures and generate tokens to sign and verify content pieces. The proposed algorithms allow the original content producer to control the content access rules by distributing tokens to authorized consumers. However, this approach requires efficient mechanisms for token renewal and group key management.

5.6 Insights & Learned Lessons

Determining access control rules for specific content independently of underlying encryption algorithms overcomes the requirement of having producers always online, so that authorized access to content can be achieved even if producers have been disconnected. The network becomes aware of the AC rules and policies as well as updates the rules for already cached contents.

The key lessons learned are the following:

- The use of broker-based mechanisms can help to enforce access rules and content security, however, the trustability of the system depends on trusting the broker node.
- Original producers may be able to update access rules even if the content is cached across the network. To this end, cache enforcement schemes are desirable to evict content associated with outdated access rules and cache content with up-to-date access rules.

- Re-encryption and broadcast-based schemes can increase the security and trust levels. However, they result in significant computation overheads and consume large amounts of in-network cache resources.

6 CHALLENGES & FUTURE RESEARCH DIRECTIONS

The main objective of this work is to collect, categorize, and analyze different access control mechanisms in NDN/ICN as well as to identify key challenges and provide potential research directions based on the presented analysis and lessons learned. In this section, we elaborate on different challenges and provide insights and possible research directions on core aspects.

6.1 Encryption-Based Access Control

Attribute-based access control mechanisms result in fine-grained policies, offering access control enforcement to a group of users. This granularity may come at the cost of having a centralized authority, probably affecting the scalability of the system. Approaches to enhance the scalability of attribute-based access control are definitely worth exploring. Name-based access control mechanisms provide semantically meaningful access control that matches the name-based nature of NDN, while identity-based access control mechanisms result in clean designs which, however, may require compute-intensive cryptographic operations. Re-encryption-based access control offers the capability to update access control rules, however, it may result in limited scalability, since it requires two or more cryptographic operations for providing authentication and updates of the rules (as already used in cloud environments [134]). Finally, broadcast-based access control provides distributed access to a group of users; however, the resulting overhead may be substantial, showcasing the need for approaches (e.g., scoped broadcast) that could mitigate the overhead. In a nutshell, further investigation is needed to optimize encryption-based access control for NDN-driven application paradigms.

6.2 Encryption-Independent Access Control

Broker-based access control results in simple designs; however, the security of the whole system relies on trusting and securing the broker. Mechanisms to identify security compromises of brokers and to establish trust with them are highly valuable. Cache enforcement access control mechanisms may contribute to enforcing the ownership and copyright rules when it comes to content cached in the network, while manifest-based access control can reduce the communication overhead and maximize the utilization of in-network caching. Similarly, interest-based access control may obfuscate content names; however, this may result in having the same content cached in the network under multiple names. This issue can be mitigated through intelligent cache management strategies which could identify multiple copies of the same content. Finally, signature-based access control may allow producers to control the content access rules by assigning access tokens to consumers. However, managing these tokens may be cumbersome, a direction that requires further research.

6.3 Dynamic Attribute-based Access Control

An attribute-based access control mechanism performs well in an ICN-based network. However, such a mechanism requires certain features to be adopted in real-world scenarios and large-scale networks. Generating dynamic attributes based on the content and type of communication is required, along with providing distributed computation rather than a proxy or a third-party entity. A possible solution might be the use of machine learning to generate attributes and Blockchain to decentralize the computation and processing [48].

6.4 Publisher-Subscriber Communication

Most of today's applications are based on a subscription model. After the subscribers register for a specific topic, generated content will be retrieved by them in an autonomous manner. Ensuring that only the authorized

subscribers receive the content is vital. Evicted subscribers should not be able to decrypt content after the eviction. At the same time, when the content may not use the provider's public key for encryption purposes, dynamically generated content based on active subscriptions may be a solution. Logical key hierarchy mechanisms can be used as an alternative solution to generate keys based on the dynamic changes of the subscription group.

6.5 Resource-Constrained Devices

IoT is considered to be the future of the Internet, where things communicate with/over the Internet using any network, any service, from any place. Most IoT sensors have limitations in computation and memory [89, 118]. To this end, lightweight access control and cryptographic mechanisms are needed for IoT devices. Directions of interest may include symmetric encryption/decryption schemes as well as evaluations of the trade-offs between security guarantees and cost. Furthermore, compute-intensive cryptographic operations can be outsourced from the resource-constrained IoT devices to powerful nodes.

6.6 In-network Cache Update Enforcement

Although in-network caching aims at enhancing network performance, decoupling the content from its original location leads to losing control of the content after its publication. The producer should be able to control and manage who is authorized to access the content even if the content is already cached in the network. Enforcing such policies is much needed in today's Internet. The use of Blockchain and other collaborative approaches may help to achieve this goal; however, a flexible trust model is required with minimal computation and overhead. Approaches based on network controllers that keep track of cached content and enforce the selected policies to the network may also be explored.

7 CONCLUSION

NDN follows session-less communication and implements content-based security where security is applied directly to the content itself rather than the communication channel. Access Control is a fundamental security requirement aiming to enforce access to content only by authorized consumers. Content naming and the decoupling of content from its original locations lead to different issues in realizing access control in NDN compared to solutions for the traditional TCP/IP network architecture [100].

In this survey, we presented and discussed a variety of access control mechanisms in NDN. We first gave an overview of the ICN paradigm, its characteristics, features, and then introduced the NDN architecture. Subsequently, we described the paradigm shift from session-based security to content-based security along with different cryptographic algorithms, security protocols, and introduction to access control. We also presented existing NDN-based access control mechanisms and classified them into different categories. Finally, we presented and identified research gaps and challenges that may be considered by the research community when designing efficient access control solutions. It is important to note that the reviewed access control mechanisms in NDN need to be seen in different contexts depending on the types of applications they are applied to. For instance, the broker-based access control mechanisms can be effective but could incur considerable overhead on the network. Similarly, the cryptographic access control (including signature-based access control) techniques are promising for non-realtime NDN applications. Further research on access control mechanisms should be conducted, especially, when we consider resource-constrained devices and publisher-subscriber communication. We hope that our work will act as a cornerstone for further research in developing efficient, viable, and effective access control mechanisms in NDN, as well as help the community to understand the trade-offs and merit of existing access control solutions.

REFERENCES

[1] 2008. 4WARD. http://www.4ward-project.eu/. Accessed: 2018-05-18.

[2] 2010. FP7 SAIL Project. http://www.sail-project.eu/. Accessed: 2018-05-18.

[3] 2019. Type-Length-Value (TLV) Encoding. https://named-data.net/doc/NDN-packet-spec/current/tlv.html

[4] Eslam G AbdAllah, Hossam S Hassanein, and Mohammad Zulkernine. 2015. A survey of security attacks in information-centric networking. *IEEE Communications Surveys & Tutorials* 17, 3 (2015), 1441–1454. https://doi.org/10.1109/COMST.2015.2392629

[5] Ibrahim Abdullahi, Suki Arif, and Suhaidi Hassan. 2015. Survey on caching approaches in Information Centric Networking. *Journal of Network and Computer Applications* 56 (2015), 48–59. https://doi.org/10.1016/j.jnca.2015.06.011

[6] Bengt Ahlgren, Christian Dannewitz, Claudio Imbrenda, Dirk Kutscher, and Borje Ohlman. 2012. A survey of information-centric networking. *IEEE Communications Magazine* 50, 7 (2012). https://doi.org/10.1109/MCOM.2012.6231276

[7] Syed Hassan Ahmed, Safdar Hussain Bouk, Dongkyun Kim, Danda B Rawat, and Houbing Song. 2017. Named data networking for software defined vehicular networks. *IEEE Communications Magazine* 55, 8 (2017), 60–66. https://doi.org/10.1109/MCOM.2017.1601137

[8] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. 2015. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials* 17, 4 (2015), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

[9] Moreno Ambrosin, Alberto Compagno, Mauro Conti, Cesar Ghali, and Gene Tsudik. 2018. Security and privacy analysis of national science foundation future internet architectures. *IEEE Communications Surveys & Tutorials* 20, 2 (2018), 1418–1442. https://doi.org/10.1109/COMST.2018.2798280

[10] Md Faizul Bari, Shihabur Rahman Chowdhury, Reaz Ahmed, Raouf Boutaba, and Bertrand Mathieu. 2012. A survey of naming and routing in information-centric networks. *IEEE Communications Magazine* 50, 12 (2012). https://doi.org/10.1109/MCOM.2012.6384450

[11] Sana Belguith, Nesrine Kaaniche, Maryline Laurent, Abderrazak Jemai, and Rabah Attia. 2018. Phoabe: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT. *Computer Networks* 133 (2018), 141–156. https://doi.org/10.1016/j.comnet.2018.01.036

[12] Ahmed Benmoussa, Abdou el Karim Tahari, Chaker Abdelaziz Kerrache, Nasreddine Lagraa, Abderrahmane Lakas, Rasheed Hussain, and Farhan Ahmad. 2020. MSIDN: Mitigation of Sophisticated Interest flooding-based DDoS attacks in Named Data Networking. *Future Generation Computer Systems* 107 (2020), 293–306. https://doi.org/10.1016/j.future.2020.01.043

[13] Cesar Bernardini, Samuel Marchal, Muhammad Rizwan Asghar, and Bruno Crispo. 2019. PrivICN: Privacy-preserving content retrieval in information-centric networking. *Computer Networks* 149 (2019), 13–28. https://doi.org/10.1016/j.comnet.2018.11.012

[14] Chaoyi Bian, Zhenkai Zhu, Alexander Afanasyev, Ersin Uzun, and Lixia Zhang. 2013. Deploying key management on NDN testbed. *Named Data Networking Project, Technical Report NDN-0009* (2013).

[15] Joakim Borgh, Edith Ngai, Börje Ohlman, and Adeel Mohammad Malik. 2017. Employing attribute-based encryption in systems with resource constrained devices in an information-centric networking context. In *Global Internet of Things Summit (GIoTS)*. IEEE, 1–6. https://doi.org/10.1109/GIOTS.2017.8016277

[16] Safdar Hussain Bouk, Syed Hassan Ahmed, Rasheed Hussain, and Yongsoon Eun. 2018. Named Data Networking's Intrinsic Cyber-Resilience for Vehicular CPS. *IEEE Access* 6 (2018), 60570–60585. https://doi.org/10.1109/ACCESS.2018.2875890

[17] Rihab Boussada, Balkis Hamdane, Mohamed Elhoucine Elhdhili, and Leila Azouz Saidane. 2019. PP-NDNoT: On preserving privacy in IoT-based E-health systems over NDN. In *IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 1–6. https://doi.org/10.1109/WCNC.2019.8886110

[18] Johannes Buchmann, Luis Carlos Coronado García, Erik Dahmen, Martin Döring, and Elena Klintsevich. 2006. CMSS–an improved Merkle signature scheme. In *International Conference on Cryptology in India*. Springer, 349–363. https://doi.org/10.1007/11941378_25

[19] Denis Butin. 2017. Hash-based signatures: State of play. *IEEE Security & Privacy* 15, 4 (2017), 37–43. https://doi.org/10.1109/MSP.2017.3151334

[20] Abdelberi Chaabane, Emiliano De Cristofaro, Mohamed Ali Kaafar, and Ersin Uzun. 2013. Privacy in content-oriented networking: Threats and countermeasures. *ACM SIGCOMM Computer Communication Review* 43, 3 (2013), 25–33. https://doi.org/10.1145/2500098.2500102

[21] Kevin Chan, Bongjun Ko, Spyridon Mastorakis, Alexander Afanasyev, and Lixia Zhang. 2017. Fuzzy interest forwarding. In *Asian Internet Engineering Conference (AINTEC)*. ACM, 31–37. https://doi.org/10.1145/3154970.3154975

[22] Tao Chen, Kai Lei, and Kuai Xu. 2014. An encryption and probability based access control model for named data networking. In *Performance Computing and Communications Conference (IPCCC), 2014 IEEE International*. IEEE, 1–8. https://doi.org/10.1109/PCCC.2014.7017100

[23] Jaeyoung Choi, Jinyoung Han, Eunsang Cho, Ted Kwon, and Yanghee Choi. 2011. A survey on content-oriented networking for efficient content delivery. *IEEE Communications Magazine* 49, 3 (2011), 121–127. https://doi.org/10.1109/MCOM.2011.5723809

[24] Roan Simões da Silva and Sergio Donizetti Zorzo. 2015. An access control mechanism to ensure privacy in named data networking using attribute-based encryption with immediate revocation of privileges. In *Annual IEEE Consumer Communications and Networking*

Conference (CCNC). IEEE, 128–133. https://doi.org/10.1109/CCNC.2015.7157958

[25] Pedro de-las Heras-Quirós, Eva M Castro, Wentao Shang, Yingdi Yu, Spyridon Mastorakis, Alexander Afanasyev, and Lixia Zhang. 2017. *The design of RoundSync protocol.* Technical Report. Technical Report. Technical Report NDN-0048, NDN.

[26] Ikram Ud Din, Suhaidi Hassan, Ahmad Almogren, Farrukh Ayub, and Mohsen Guizani. 2019. PUC: Packet Update Caching for energy efficient IoT-based Information-Centric Networking. *Future Generation Computer Systems* (2019). https://doi.org/10.1016/j.future.2019.11.022

[27] Ikram Ud Din, Suhaidi Hassan, Muhammad Khurram Khan, Mohsen Guizani, Osman Ghazali, and Adib Habbal. 2018. Caching in Information-Centric Networking: Strategies, Challenges, and Future Research Directions. *IEEE Communications Surveys & Tutorials* 20, 2 (2018), 1443–1474. https://doi.org/10.1109/COMST.2017.2787609

[28] Chao Fang, F Richard Yu, Tao Huang, Jiang Liu, and Yunjie Liu. 2015. A survey of green information-centric networking: Research issues and challenges. *IEEE Communications Surveys & Tutorials* 17, 3 (2015), 1455–1472. https://doi.org/10.1109/COMST.2015.2394307

[29] Yuan Fei, Huibiao Zhu, and Phan Cong Vinh. 2020. Security analysis of the access control solution of NDN using BAN logic. *Mobile Networks and Applications* (2020), 1–12. https://doi.org/10.1007/s11036-019-01435-z

[30] Tao Feng and Jiaqi Guo. 2018. A New Access Control System Based on CP-ABE in Named Data Networking. *IJ Network Security* 20, 4 (2018), 710–720.

[31] Nikos Fotiou and Bander A Alzahrani. 2018. Rendezvous-based access control for information-centric architectures. *International Journal of Network Management* 28, 1 (2018), e2007. https://doi.org/10.1002/nem.2007

[32] Nikos Fotiou, Giannis F Marias, and George C Polyzos. 2012. Access control enforcement delegation for information-centric networking architectures. *ACM SIGCOMM Computer Communication Review* 42, 4 (2012), 497–502. https://doi.org/10.1145/2377677.2377773

[33] Nikos Fotiou, Pekka Nikander, Dirk Trossen, and George C Polyzos. 2010. Developing Information Networking Further: From PSIRP to PURSUIT. In *Conference on Broadband*. Springer, 1–13. https://doi.org/10.1007/978-3-642-30376-0_1

[34] Nikos Fotiou and George C Polyzos. 2016. Decentralized name-based security for content distribution using blockchains. In *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 415–420. https://doi.org/10.1109/INFCOMW.2016.7562112

[35] Wenliang Fu, Hila Ben Abraham, and Patrick Crowley. 2015. Synchronizing namespaces with invertible bloom filters. In *ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS)*. IEEE, 123–134. https://doi.org/10.1109/ANCS.2015.7110126

[36] Wenliang Fu, Hila Ben Abraham, and Patrick Crowley. 2014. iSync: a high performance and scalable data synchronization protocol for named data networking. In *ACM Conference on Information-Centric Networking*. 181–182. https://doi.org/0.1145/2660129.2660161

[37] G. Garcia, A. Beben, F. J. Ramon, A. Maeso, I. Psaras, G. Pavlou, et al. 2011. COMET: Content Mediator Architecture for Content-aware Networks. In *Future Network Mobile Summit*.

[38] Cesar Ghali, Marc A. Schlosberg, Gene Tsudik, and Christopher A. Wood. 2015. Interest-Based Access Control for Content Centric Networks. In *ACM Conference on Information-Centric Networking*. ACM, 147–156. https://doi.org/10.1145/2810156.2810174

[39] Cesar Ghali, Gene Tsudik, and Ersin Uzun. 2019. In Content We Trust: Network-Layer Trust in Content-Centric Networking. *IEEE/ACM Transactions on Networking* 27, 5 (2019), 1787–1800. https://doi.org/10.1109/TNET.2019.2926320

[40] Cesar Ghali, Gene Tsudik, and Christopher A Wood. 2017. When encryption is not enough: privacy attacks in content-centric networking. In *ACM Conference on Information-Centric Networking*. ACM, 1–10. https://doi.org/10.1145/3125719.3125723

[41] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. 2006. Attribute-based encryption for fine-grained access control of encrypted data. In *ACM conference on Computer and Communications Security (CCS)*. ACM, 89–98. https://doi.org/10.1145/1180405.1180418

[42] Dennis Grewe, KP Pavithra Rao, Sebastian Schildt, Marco Wagner, Dominik Schoop, and Hannes Frey. 2017. EnCIRCLE: Encryption-based access control for information-centric connected vehicles. In *International Conference on the Network of the Future (NOF)*. IEEE, 114–119. https://doi.org/10.1109/NOF.2017.8251229

[43] Balkis Hamdane and Sihem Guemara El Fatmi. 2015. A credential and encryption based access control solution for named data networking. In *IFIP/IEEE International Symposium on Integrated Network Management (IM)*. IEEE, 1234–1237. https://doi.org/10.1109/INM.2015.7140473

[44] Balkis Hamdane, Mounira Msahli, Ahmed Serhrouchni, and Sihem Guemara El Fatmi. 2013. Data-based access control in named data networking. In *IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*. IEEE, 531–536. https://doi.org/10.4108/icst.collaboratecom.2013.254180

[45] Balkis Hamdane, Ahmed Serhrouchni, and Sihem Guemara El Fatmi. 2013. Access control enforcement in named data networking. In *International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, 576–581. https://doi.org/10.1109/ICITST.2013.6750268

[46] Rasheed Hussain, Safdar H Bouk, Nadeem Javaid, Adil M Khan, and Jooyoung Lee. 2018. Realization of VANET-Based Cloud Services through Named Data Networking. *IEEE Communications Magazine* 56, 8 (2018), 168–175. https://doi.org/10.1109/MCOM.2018.1700514

[47] Mihaela Ion, Jianqing Zhang, and Eve M Schooler. 2013. Toward content-centric privacy in ICN: Attribute-based encryption and routing. In *ACM SIGCOMM workshop on Information-centric networking*. ACM, 39–40. https://doi.org/10.1145/2534169.2491717

[48] Mian Ahmad Jan, Jinjin Cai, Xiang-Chuan Gao, Fazlullah Khan, Spyridon Mastorakis, Muhammad Usman, Mamoun Alazab, and Paul Watters. 2020. Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges and future directions. *Journal of Network and Computer Applications* (2020), 102918.

[49] Xiaoke Jiang, Jun Bi, Guoshun Nan, and Zhaogeng Li. 2015. A survey on information-centric networking: rationales, designs and debates. *China Communications* 12, 7 (2015), 1–12. https://doi.org/10.1109/CC.2015.7188520

[50] Yinhao Jiang, Willy Susilo, Yi Mu, and Fuchun Guo. 2018. Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing. *Future Generation Computer Systems* 78 (2018), 720–729. https://doi.org/10.1016/j.future.2017.01.026

[51] Ioanna Angeliki Kapetanidou, Christos-Alexandros Sarros, and Vassilis Tsaoussidis. 2019. Reputation-Based Trust Approaches in Named Data Networking. *Future Internet* (2019), 11–241. Issue 11. https://doi.org/10.3390/fi11110241

[52] Hakima Khelifi, SenLin Luo, Boubakr Nour, and Hassine Moungla. 2019. A Name-to-Hash Encoding Scheme for Vehicular Named Data Networks. In *International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 1–6. https://doi.org/10.1109/IWCMC.2019.8766564

[53] Hakima Khelifi, SenLin Luo, Boubakr Nour, and Hassine Moungla. 2019. LQCC: A Link Quality-based Congestion Control Scheme in Named Data Networks. In *IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 1–6.

[54] Hakima Khelifi, Senlin Luo, Boubakr Nour, and Hassine Moungla. 2019. A QoS-aware Cache Replacement Policy for Vehicular Named Data Networks. In *IEEE Global Communications Conference (GLOBECOM)*. IEEE, 1–6.

[55] H. Khelifi, S. Luo, B. Nour, and H. Moungla. 2020. In-Network Caching in ICN-based Vehicular Networks: Effectiveness & Performance Evaluation. In *IEEE International Conference on Communications (ICC)*. IEEE, 1–6. https://doi.org/10.1109/ICC40277.2020.9148950

[56] H. Khelifi, S. Luo, B. Nour, H. Moungla, SH. Ahmed, and M. Guizani. 2020. A Blockchain-based Architecture for Secure Vehicular Named Data Networks. *Computers & Electrical Engineering* 86 (2020), 106715. https://doi.org/10.1016/j.compeleceng.2020.106715

[57] Hakima Khelifi, Senlin Luo, Boubakr Nour, Hassine Moungla, and Syed Hassan Ahmed. 2018. Reputation-based Blockchain for Secure NDN Caching in Vehicular Networks. In *IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 1–6. https://doi.org/10.1109/CSCN.2018.8581849

[58] Hakima Khelifi, Senlin Luo, Boubakr Nour, Hassine Moungla, Yasir Faheem, Rasheed Hussain, and Adlen Ksentini. 2019. Named Data Networking in Vehicular Ad hoc Networks: State-of-the-Art and Challenges. *IEEE Communications Surveys and Tutorials* (2019). https://doi.org/10.1109/COMST.2019.2894816

[59] Hakima Khelifi, Senlin Luo, Boubakr Nour, Akrem Sellami, Hassine Moungla, Syed Hassan Ahmed, and Mohsen Guizani. 2019. Bringing Deep Learning at The Edge of Information-Centric Internet of Things. *IEEE Communications Letters* 23, 1 (2019), 52–55. https://doi.org/10.1109/LCOMM.2018.2875978

[60] Hakima Khelifi, Senlin Luo, Boubakr Nour, Akrem Sellami, Hassine Moungla, and F. Naït-Abdesselam. 2018. An Optimized Proactive Caching Scheme based on Mobility Prediction for Vehicular Networks. In *IEEE Global Communications Conference (GLOBECOM)*. IEEE, 1–6. https://doi.org/10.1109/GLOCOM.2018.8647898

[61] Hakima Khelifi, Senlin Luo, Boubakr Nour, and Chhattan Shah Shah. 2018. Security and Privacy Issues in Vehicular Named Data Networks: An Overview. *Mobile Information Systems* 2018 (Sep 2018), 1–11. https://doi.org/10.1155/2018/5672154

[62] Teemu Koponen, Mohit Chawla, Byung-Gon Chun, Andrey Ermolinskiy, Kye Hyun Kim, Scott Shenker, and Ion Stoica. 2007. A data-oriented (and beyond) network architecture. In *ACM SIGCOMM Computer Communication Review*, Vol. 37. ACM, 181–192.

[63] Michał Król, Spyridon Mastorakis, David Oran, and Dirk Kutscher. 2019. Compute First Networking: Distributed Computing meets ICN. In *ACM Conference on Information-Centric Networking*. ACM, 67–77. https://doi.org/10.1145/3357150.3357395

[64] Jun Kurihara, Kenji Yokota, and Atsushi Tagami. 2016. A consumer-driven access control approach to censorship circumvention in content-centric networking. In *ACM Conference on Information-Centric Networking*. ACM, 186–194. https://doi.org/10.1145/2984356.2984360

[65] Jun Kuriharay, Ersin Uzun, and Christopher A Wood. 2015. An encryption-based access control framework for content-centric networking. In *IFIP Networking Conference (IFIP Networking)*. IEEE, 1–9. https://doi.org/10.1109/IFIPNetworking.2015.7145300

[66] Dirk Kutscher, Suyong Eum, Kostas Pentikousis, Ioannis Psaras, Daniel Corujo, Damien Saucez, Thomas C. Schmidt, and Matthias Wählisch. 2016. Information-Centric Networking (ICN) Research Challenges. RFC 7927. https://doi.org/10.17487/RFC7927

[67] Bing Li, Dijiang Huang, Zhijie Wang, and Yan Zhu. 2018. Attribute-based access control for ICN naming scheme. *IEEE Transactions on Dependable and Secure Computing* 15, 2 (2018), 194–206. https://doi.org/10.1109/TDSC.2016.2550437

[68] Bing Li, Zhijie Wang, Dijiang Huang, and Yan Zhu. 2014. *Toward privacy-preserving content access control for information centric networking*. Technical Report. Arizona State Univ Tempe Office of Research and Sponsored Project Administration.

[69] Jiguo Li, Qihong Yu, Yichen Zhang, and Jian Shen. 2019. Key-policy attribute-based encryption against continual auxiliary input leakage. *Information Sciences* 470 (2019), 175–188. https://doi.org/10.1016/j.ins.2018.07.077

[70] Qi Li, Xinwen Zhang, Qingji Zheng, Ravi Sandhu, and Xiaoming Fu. 2015. LIVE: Lightweight integrity verification and content access control for named data networking. *IEEE Transactions on Information Forensics and Security* 10, 2 (2015), 308–320. https:

//doi.org/10.1109/TIFS.2014.2365742

[71] Tianxiang Li, Zhaoning Kong, Spyridon Mastorakis, and Lixia Zhang. 2019. Distributed Dataset Synchronization in Disruptive Networks. In *IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*. IEEE, 428–437.

[72] Tianxiang Li, Spyridon Mastorakis, Xin Xu, Haitao Zhang, and Lixia Zhang. 2018. Data synchronization in Ad Hoc mobile networks. In *Proceedings of the 5th ACM Conference on Information-Centric Networking*. 186–187. https://doi.org/10.1145/3267955.3269024

[73] Zhuo Li, Yaping Xu, Beichuan Zhang, Liu Yan, and Kaihua Liu. 2019. Packet Forwarding in Named Data Networking Requirements and Survey of Solutions. *IEEE Communications Surveys & Tutorials* 21, 2 (2019), 1950–1987. https://doi.org/10.1109/COMST.2018.2880444

[74] Teng Liang, Ju Pan, and Beichuan Zhang. 2018. NDNizing Existing Applications: Research Issues and Experiences. In *ACM Conference on Information-Centric Networking*. ACM, 1–10. https://doi.org/10.1145/3267955.3267969

[75] Ningchun Liu, Shuai Gao, and Ningho Hou. 2019. CDAC: A Collaborative Data Access Control Scheme in Named Data Networking. In *International Conference on Hot Information-Centric Networking (HotICN)*. IEEE, 44–49. https://doi.org/10.1109/HotICN48464.2019.9063206

[76] Roman Lutz. 2016. Security and privacy in future internet architectures-benefits and challenges of content centric networks. *arXiv preprint arXiv:1601.01278* (2016).

[77] Qiuyun Lyu, Yizhen Qi, Xiaochen Zhang, Huaping Liu, Qiuhua Wang, and Ning Zheng. 2020. SBAC: A secure blockchain-based access control framework for information-centric networking. *Journal of Network and Computer Applications* 149 (2020), 102444. https://doi.org/10.1016/j.jnca.2019.102444

[78] Manisha Malik, Maitreyee Dutta, and Jorge Granjal. 2019. A Survey of Key Bootstrapping Protocols Based on Public Key Cryptography in the Internet of Things. *IEEE Access* 7 (2019), 27443–27464. https://doi.org/10.1109/ACCESS.2019.2900957

[79] Michele Mangili, Fabio Martignon, and Stefano Paraboschi. 2015. A cache-aware mechanism to enforce confidentiality, trackability and access policy evolution in content-centric networks. *Computer Networks* 76 (2015), 126–145. https://doi.org/10.1016/j.comnet.2014.11.010

[80] Claudio Marxer, Christopher Scherb, and Christian Tschudin. 2016. Access-controlled in-network processing of named data. In *ACM Conference on Information-Centric Networking*. ACM, 77–82. https://doi.org/10.1145/2984356.2984366

[81] Claudio Marxer and Christian Tschudin. 2017. Schematized access control for data cubes and trees. In *ACM Conference on Information-Centric Networking*. ACM, 170–175. https://doi.org/10.1145/3125719.3125736

[82] Spyridon Mastorakis. 2019. *Peer-to-peer data sharing in named data networking*. Ph.D. Dissertation. UCLA.

[83] Spyridon Mastorakis, Alexander Afanasyev, Yingdi Yu, and Lixia Zhang. 2017. nTorrent: Peer-to-peer file sharing in named data networking. In *International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 1–10. https://doi.org/10.1109/ICCCN.2017.8038462

[84] Spyridon Mastorakis, Kevin Chan, Bongjun Ko, Alexander Afanasyev, and Lixia Zhang. 2018. Experimentation with fuzzy interest forwarding in named data networking. *arXiv preprint arXiv:1802.03072* (2018).

[85] Spyridon Mastorakis, Peter Gusev, Alexander Afanasyev, and Lixia Zhang. 2018. Real-Time Data Retrieval in Named Data Networking. In *IEEE International Conference on Hot Information-Centric Networking (HotICN)*. IEEE, 61–66. https://doi.org/10.1109/HOTICN.2018.8605992

[86] Spyridon Mastorakis, Tianxiang Li, and Lixia Zhang. 2020. DAPES: Named Data for Off-the-Grid File Sharing with Peer-to-Peer Interactions. *arXiv preprint arXiv:2006.01651* (2020).

[87] Spyridon Mastorakis and Abderrahmen Mtibaa. 2019. Towards Service Discovery and Invocation in Data-Centric Edge Networks. In *IEEE International Conference on Network Protocols (ICNP)*. IEEE, 1–6. https://doi.org/10.1109/ICNP.2019.8888081

[88] Spyridon Mastorakis, Abderrahmen Mtibaa, Jonathan Lee, and Satyajayant Misra. 2020. ICedge: When Edge Computing Meets Information-Centric Networking. *IEEE Internet of Things Journal* 7, 5 (2020), 4203–4217. https://doi.org/10.1109/JIOT.2020.2966924

[89] Spyridon Mastorakis, Xin Zhong, Pei-Chi Huang, and Reza Tourani. 2020. DLWIoT: Deep Learning-based Watermarking for Authorized IoT Onboarding. *arXiv preprint arXiv:2010.10334* (2020).

[90] Mohamed Nidhal Mejri and Jalel Ben-Othman. 2016. GDVAN: a new greedy behavior attack detection algorithm for VANETs. *IEEE Transactions on Mobile Computing* 16, 3 (2016), 759–771. https://doi.org/10.1109/TMC.2016.2577035

[91] Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. 2014. Survey on VANET security challenges and possible cryptographic solutions. *Vehicular Communications* 1, 2 (2014), 53–66. https://doi.org/10.1016/j.vehcom.2014.05.001

[92] N. Blefari Melazzi, S. Salsano, A. Detti, G. Tropea, L. Chiariglione, A. Difino, et al. 2012. Publish/subscribe over information centric networks: A Standardized approach in CONVERGENCE. In *Future Network Mobile Summit*.

[93] Satyajayant Misra, Reza Tourani, and Nahid Ebrahimi Majd. 2013. Secure content delivery in information-centric networks: Design, implementation, and analyses. In *ACM SIGCOMM workshop on Information-Centric Networking*. ACM, 73–78. https://doi.org/10.1145/2491224.2491228

[94] Satyajayant Misra, Reza Tourani, Frank Natividad, Travis Mick, Nahid Ebrahimi Majd, and Hong Huang. 2019. AccConF: An access control framework for leveraging in-network cached data in the ICN-enabled wireless edge. *IEEE Transactions on Dependable and Secure Computing* 16, 1 (2019), 5–17. https://doi.org/10.1109/TDSC.2017.2672991

[95] Lynda Mokdad, Jalel Ben-Othman, and Anh Tuan Nguyen. 2015. DJAVAN: Detecting jamming attacks in Vehicle Ad hoc Networks. *Performance Evaluation* 87 (2015), 47–59. https://doi.org/10.1016/j.peva.2015.01.003

[96] Edith Ngai, Börje Ohlman, Gene Tsudik, Ersin Uzun, Matthias Wählisch, and Christopher A Wood. 2017. Can we make a cake and eat it too? A discussion of ICN security and privacy. *ACM SIGCOMM Computer Communication Review* 47, 1 (2017), 49–54.

[97] B. Nour, H. Ibn Khedher, H. Moungla, H. Afifi, F. Li, K. Sharif, H. Khelifi, and M. Guizani. 2020. Internet of Things Mobility over Information-Centric/Named-Data Networking. *IEEE Internet Computing* 24, 1 (2020), 14–24. https://doi.org/10.1109/MIC.2019.2963187

[98] B. Nour, H. Khelifi, R. Hussain, H. Moungla, , and S. H. Bouk. 2020. A Collaborative Multi-Metric Interface Ranking Scheme for Named Data Networks. In *International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 2088–2093. https://doi.org/10.1109/IWCMC48107.2020.9148196

[99] B. Nour, H. Khelifi, H. Moungla, R. Hussain, and N. Guizani. 2020. A Distributed Cache Placement Scheme for Large-Scale ICN Networks. *IEEE Network* 34, 6 (2020), 126–132. https://doi.org/10.1109/MNET.011.2000081

[100] B. Nour, F. Li, H. Khelifi, H. Moungla, and A. Ksentini. 2019. Coexistence of ICN and IP Networks: An NFV as a Service Approach. In *IEEE Global Communications Conference (GLOBECOM)*. IEEE, 1–6. https://doi.org/10.1109/GLOBECOM38437.2019.9013881

[101] Boubakr Nour, Spyridon Mastorakis, and Abderrahmen Mtibaa. 2020. Compute-less networking: Perspectives, challenges, and opportunities. *IEEE Network* (2020).

[102] B. Nour, K. Sharif, F. Li, S. Biswas, H. Moungla, M. Guizani, and Y. Wang. 2019. A Survey of Internet of Things Communication using ICN: A Use Case Perspective. *Computer Communications* (2019). https://doi.org/10.1016/j.comcom.2019.05.010

[103] Boubakr Nour, Kashif Sharif, Fan Li, Hakima Khelifi, and Hassine Moungla. 2018. NNCP: A Named Data Network Control Protocol for IoT Applications. In *IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 1–6. https://doi.org/10.1109/CSCN.2018.8581844

[104] Boubakr Nour, Kashif Sharif, Fan Li, and Hassine Moungla. 2017. A Distributed ICN-based IoT Network Architecture: An Ambient Assisted Living Application Case Study. In *IEEE Global Communications Conference (GLOBECOM)*. IEEE, 1–6. https://doi.org/10.1109/GLOCOM.2017.8255022

[105] Boubakr Nour, Kashif Sharif, Fan Li, Hassine Moungla, Ahmed E. Kamal, and Hossam Afifi. 2018. NCP: A Near ICN Cache Placement Scheme for IoT-based Traffic Class. In *IEEE Global Communications Conference (GLOBECOM)*. IEEE, 1–6. https://doi.org/10.1109/GLOCOM.2018.8647629

[106] Boubakr Nour, Kashif Sharif, Fan Li, Hassine Moungla, and Yang Liu. 2017. M2HAV: A Standardized ICN Naming Scheme for Wireless Devices in Internet of Things. In *International Conference Wireless Algorithms, Systems, and Applications (WASA)*. Springer International Publishing, 289–301. https://doi.org/10.1007/978-3-319-60033-8_26

[107] B. Nour, K. Sharif, F. Li, H. Moungla, and Y. Liu. 2019. A Unified Hybrid Information-Centric Naming Scheme for IoT Applications. *Computer Communications* 150 (Nov 2019), 103–114. https://doi.org/10.1016/j.comcom.2019.11.020

[108] Boubakr Nour, K. Sharif, F. Li, H. Moungla, and Y. Liu. 2019. A Unified Hybrid Information-Centric Naming Scheme for IoT Applications. *Computer Communications* (Nov 2019). https://doi.org/10.1016/j.comcom.2019.11.020

[109] Boubakr Nour, Kashif Sharif, Fan Li, and Yu Wang. 2019. Security and Privacy Challenges in Information Centric Wireless IoT Networks. *IEEE Security & Privacy* (2019). https://doi.org/10.1109/MSEC.2019.2925337

[110] Boubakr Nour, Kashif Sharif, Fan Li, Song Yang, Hassine Moungla, and Yu Wang. 2019. ICN Publisher-Subscriber Models: Challenges and Group-based Communication. *IEEE Network* (2019). https://doi.org/10.1109/MNET.2019.1800551

[111] Fabian Oehlmann. 2013. Content-Centric Networking. *Seminar FI & IITM: Network Architectures and Services* 43 (2013), 11–18. https://doi.org/10.2312/NET-2013-02-1_06

[112] Svetlana Ostrovskaya, Oleg Surnin, Rasheed Hussain, Safdar Hussain Bouk, JooYoung Lee, Narges Mehran, Syed Hassan Ahmed, and Abderrahim Benslimane. 2018. Towards Multi-metric Cache Replacement Policies in Vehicular Named Data Networks. In *IEEE Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 1–7. https://doi.org/10.1109/PIMRC.2018.8580741

[113] Jianli Pan, Subharthi Paul, and Raj Jain. 2011. A survey of the research on future internet architectures. *IEEE Communications Magazine* 49, 7 (2011). https://doi.org/10.1109/MCOM.2011.5936152

[114] Kostas Pentikousis, Börje Ohlman, Elwyn B. Davies, Spiros Spirou, and Gennaro Boggia. 2016. Information-Centric Networking: Evaluation and Security Considerations. RFC 7945. https://doi.org/10.17487/RFC7945

[115] Lei Pi and Lan Wang. 2018. Secure bootstrapping and access control in NDN-based smart home systems. In *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 1–2. https://doi.org/10.1109/INFCOMW.2018.8407000

[116] Akbar Rahman, Dirk Trossen, Dirk Kutscher, and Ravi Ravindran. 2019. *Deployment Considerations for Information-Centric Networking (ICN)*. Internet-Draft. Internet Engineering Task Force. Work in Progress.

[117] Sanjeev Kaushik Ramani, Reza Tourani, George Torres, Satyajayant Misra, and Alexander Afanasyev. 2019. NDN-ABS: Attribute-Based Signature Scheme for Named Data Networking. In *ACM Conference on Information-Centric Networking*. 123–133. https://doi.org/10.1145/3357150.3357393

[118] Muhammad Atif Ur Rehman, Rehmat Ullah, Byung-Seo Kim, Boubakr Nour, and Spyridon Mastorakis. 2020. CCIC-WSN: An Architecture for Single Channel Cluster-based Information-Centric Wireless Sensor Networks. *IEEE Internet of Things Journal* (2020).

[119] P. H. Rettore, G. Maia, L. A. Villas, and A. A. F. Loureiro. 2019. Vehicular Data Space: The Data Point of View. *IEEE Communications Surveys Tutorials* (2019), 1–1. https://doi.org/10.1109/COMST.2019.2911906

[120] Daniel Rezende, Carlos Maziero, and Elisa Mannes. 2018. A distributed online certificate status protocol for named data networks. In *Annual ACM Symposium on Applied Computing*. ACM, 2102–2108. https://doi.org/10.1145/3167132.3167358

[121] Divya Saxena, Vaskar Raychoudhury, Neeraj Suri, Christian Becker, and Jiannong Cao. 2016. Named data networking: a survey. *Computer Science Review* 19 (2016), 15–55. https://doi.org/10.1016/j.cosrev.2016.01.001

[122] Anand Seetharam. 2018. On Caching and Routing in Information-Centric Networks. *IEEE Communications Magazine* 56, 3 (2018), 204–209. https://doi.org/10.1109/MCOM.2017.1700184

[123] O. Serhane, K. Yahyaoui, B. Nour, , and H. Moungla. 2020. A Label-based Producer Mobility Support in 5G-enabled ICN Networks. In *International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 2094–2099. https://doi.org/10.1109/IWCMC48107.2020.9148578

[124] O. Serhane, K. Yahyaoui, B. Nour, and H. Moungla. 2020. CnS: A Cache and Split Scheme for 5G-enabled ICN Networks. In *IEEE International Conference on Communications (ICC)*. IEEE, 1–6. https://doi.org/10.1109/ICC40277.2020.9149332

[125] Ivan Seskar, Kiran Nagaraja, Sam Nelson, and Dipankar Raychaudhuri. 2011. Mobilityfirst: Future Internet Architecture Project. In *Asian Internet Engineering Conference*. ACM. https://doi.org/10.1145/2089016.2089017

[126] Masoumeh Shafieinejad and Reihaneh Safavi-Naini. 2017. A Post-Quantum One Time Signature Using Bloom Filter. In *Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 397–3972. https://doi.org/10.1109/PST.2017.00056

[127] Wentao Shang, Yingdi Yu, Lijing Wang, Alexander Afanasyev, and Lixia Zhang. 2017. *A Survey of Distributed Dataset Synchronization in Named Data Networking*. Technical Report. Technical Report NDN-0053, NDN.

[128] Susmit Shannigrahi, Chengyu Fan, and Christos Papadopoulos. 2018. SCARI: A Strategic Caching and Reservation Protocol for ICN. In *Proceedings of the Asian Internet Engineering Conference*. ACM, 1–8. https://doi.org/10.1145/3289166.3289167

[129] Justine Sherry, Chang Lan, Raluca Ada Popa, and Sylvia Ratnasamy. 2015. Blindbox: Deep packet inspection over encrypted traffic. *ACM SIGCOMM Computer communication review* 45, 4 (2015), 213–226. https://doi.org/10.1145/2785956.2787502

[130] Weisong Shi, Jie Cao, Quan Zhang, Youhuizi Li, and Lanyu Xu. 2016. Edge computing: Vision and challenges. *IEEE Internet of Things Journal* 3, 5 (2016), 637–646. https://doi.org/10.1109/JIOT.2016.2579198

[131] Sapna Singh. 2012. A trust based approach for secure access control in information centric network. *International Journal of Information and Network Security* 1, 2 (2012), 97. https://doi.org/10.11591/ijins.v1i2.467

[132] Junggab Son, Donghyun Kim, Md Zakirul Alam Bhuiyan, Rasheed Hussain, and Heekuck Oh. 2017. A new outsourcing conditional proxy re-encryption suitable for mobile cloud environment. *Concurrency and Computation: Practice and Experience* 29, 14 (2017), e3946. https://doi.org/10.1002/cpe.3946

[133] J. Son, D. Kim, R. Hussain, and H. Oh. 2014. Conditional proxy re-encryption for secure big data group sharing in cloud environment. In *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 541–546. https://doi.org/10.1109/INFCOMW.2014.6849289

[134] J. Son, D. Kim, R. Hussain, and H. Oh. 2014. Conditional proxy re-encryption for secure big data group sharing in cloud environment. In *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 541–546. https://doi.org/10.1109/INFCOMW.2014.6849289

[135] Kalika Suksomboon, Atsushi Tagami, Anirban Basu, and Jun Kurihara. 2017. IPRES: In-device proxy re-encryption service for secure ICN. In *ACM Conference on Information-Centric Networking*. ACM, 176–177. https://doi.org/10.1145/3125719.3132089

[136] Xiaobin Tan, Zifei Zhou, Cliff Zou, Yukun Niu, and Xin Chen. 2014. Copyright protection in named data networking. In *International Conference on Wireless Communications and Signal Processing (WCSP)*. IEEE, 1–6. https://doi.org/10.1109/WCSP.2014.6992077

[137] Reza Tourani, Travis Mick, Satyajayant Misra, and Gaurav Panwar. 2018. Security, privacy, and access control in information-centric networking: A survey. *IEEE Communications Surveys & Tutorials* 20, 1 (2018), 566–600. https://doi.org/10.1109/COMST.2017.2749508

[138] Christian Tschudin. 2016. Private Information Retrieval over ICN. In *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 534–539. https://doi.org/10.1109/INFCOMW.2016.7562134

[139] Christian Tschudin, Ersin Uzun, and Christopher A Wood. 2016. Trust in information-centric networking: From theory to practice. In *International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 1–9. https://doi.org/10.1109/ICCCN.2016.7568589

[140] Yi-Fan Tseng, Chun-I Fan, and Chin-Yu Wu. 2018. FGAC-NDN: Fine-Grained Access Control for Named Data Networks. *IEEE Transactions on Network and Service Management* 16, 1 (2018), 143–152. https://doi.org/10.1109/TNSM.2018.2864330

[141] Gene Tsudik, Ersin Uzun, and Christopher A Wood. 2016. AC3N: Anonymous communication in Content-Centric Networking. In *IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 988–991. https://doi.org/10.1109/CCNC.2016.7444924

[142] Gareth Tyson, Nishanth Sastry, Ivica Rimac, Ruben Cuevas, and Andreas Mauthe. 2012. A survey of mobility in information-centric networks: Challenges and research directions. In *ACM Workshop on Emerging Name-Oriented Mobile Networking Design-Architecture, Algorithms, and Applications*. 1–6. https://doi.org/10.1145/2248361.2248363

[143] Rehmat Ullah, Syed Hassan Ahmed, and Byung-Seo Kim. 2018. Information-Centric Networking With Edge Computing for IoT: Research Challenges and Future Directions. *IEEE Access* 6 (2018), 73465–73488. https://doi.org/10.1109/ACCESS.2018.2884536

[144] Rehmat Ullah, Muhammad Atif Ur Rehman, Muhammad Ali Naeem, Byung-Seo Kim, and Spyridon Mastorakis. 2020. ICN with edge for 5G: Exploiting in-network caching in ICN-based edge computing for 5G networks. *Future Generation Computer Systems* (2020).

[145] Henk CA Van Tilborg and Sushil Jajodia. 2014. *Encyclopedia of cryptography and security*. Springer Science & Business Media.

[146] Athanasios V Vasilakos, Zhe Li, Gwendal Simon, and Wei You. 2015. Information centric network: Research challenges and opportunities. *Journal of network and computer applications* 52 (2015), 1–10. https://doi.org/10.1016/j.jnca.2015.02.001

[147] Anna Volkova, Michael Niedermeier, Robert Basmadjian, and Hermann de Meer. 2019. Security Challenges in Control Network Protocols: A Survey. *IEEE Communications Surveys & Tutorials* 21, 1 (2019), 619–639. https://doi.org/10.1109/COMST.2018.2872114

[148] Satyanarayana Vusirikala, Spyridon Mastorakis, Alexander Afanasyev, and Lixia Zhang. 2016. Hop-by-hop best effort link layer reliability in named data networking. *NDN, Technical Report NDN-0041* (2016).

[149] Licheng Wang, Zonghua Zhang, Mianxiong Dong, Lihua Wang, Zhenfu Cao, and Yixian Yang. 2018. Securing Named Data Networking: Attribute-Based Encryption and Beyond. *IEEE Communications Magazine* 56, 11 (2018), 76–81. https://doi.org/10.1109/MCOM.2018.1701123

[150] Yu Wang, Mingwei Xu, Zhen Feng, Qing Li, and Qi Li. 2014. Session-based access control in information-centric networks: Design and analyses. In *IEEE International Performance Computing and Communications Conference (IPCCC)*. IEEE, 1–8. https://doi.org/10.1109/PCCC.2014.7017094

[151] Christopher A Wood and Ersin Uzun. 2014. Flexible end-to-end content security in CCN. In *IEEE Consumer Communications and Networking Conference (CCNC)*. IEEE, 858–865. https://doi.org/10.1109/CCNC.2014.6940528

[152] Zhijun Wu, Enzhong Xu, Liang Liu, and Meng Yue. 2019. CHTDS: A CP-ABE Access Control Scheme Based on Hash Table and Data Segmentation in NDN. In *IEEE International Conference On Trust, Security And Privacy In Computing And Communications/IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 843–848. https://doi.org/10.1109/TrustCom/BigDataSE.2019.00122

[153] Zhijun Wu, Yun Zhang, and Enzhong Xu. 2020. Multi-Authority Revocable Access Control Method Based on CP-ABE in NDN. *Future Internet* 12, 1 (2020), 15. https://doi.org/10.3390/fi12010015

[154] Chengcheng Xu, Shuhui Chen, Jinshu Su, Siu-Ming Yiu, and Lucas CK Hui. 2016. A survey on regular expression matching for deep packet inspection: Applications, algorithms, and hardware platforms. *IEEE Communications Surveys & Tutorials* 18, 4 (2016), 2991–3029. https://doi.org/10.1109/COMST.2016.2566669

[155] Kaiping Xue, Peixuan He, Xiang Zhang, Qiudong Xia, David SL Wei, Hao Yue, and Feng Wu. 2019. A Secure, Efficient, and Accountable Edge-Based Access Control Framework for Information Centric Networks. *IEEE/ACM Transactions on Networking* 27, 3 (2019), 1220–1233. https://doi.org/10.1109/TNET.2019.2914189

[156] George Xylomenos, Christopher N Ververidis, Vasilios A Siris, Nikos Fotiou, Christos Tsilopoulos, Xenofon Vasilakos, Konstantinos V Katsaros, and George C Polyzos. 2014. A survey of information-centric networking research. *IEEE Communications Surveys & Tutorials* 16, 2 (2014), 1024–1049. https://doi.org/10.1109/SURV.2013.070813.00063

[157] Haomiao Yang, Xiaofen Wang, Chun Yang, Xin Cong, and You Zhang. 2019. Securing content-centric networks with content-based encryption. *Journal of Network and Computer Applications* 128 (2019), 21–32. https://doi.org/10.1016/j.jnca.2018.12.005

[158] Yingdi Yu, Alexander Afanasyev, and Lixia Zhang. 2015. Name-based access control. *Named Data Networking Project, Technical Report NDN-0034* (2015).

[159] Yong Yu, Yannan Li, Xiaojiang Du, Ruonan Chen, and Bo Yang. 2018. Content Protection in Named Data Networking: Challenges and Potential Solutions. *IEEE Communications Magazine* 56, 11 (2018), 82–87. https://doi.org/10.1109/MCOM.2018.1701086

[160] Guoqiang Zhang, Yang Li, and Tao Lin. 2013. Caching in information centric networking: A survey. *Computer Networks* 57, 16 (2013), 3128–3141. https://doi.org/10.1016/j.comnet.2013.07.007

[161] Lixia Zhang, Alexander Afanasyev, Jeffrey Burke, Van Jacobson, Patrick Crowley, Christos Papadopoulos, Lan Wang, Beichuan Zhang, et al. 2014. Named Data Networking. *ACM SIGCOMM Computer Communication Review* 44, 3 (2014), 66–73. https://doi.org/10.1145/2656877.2656887

[162] Lixia Zhang, Deborah Estrin, Jeffrey Burke, Van Jacobson, James D Thornton, Diana K Smetters, Beichuan Zhang, Gene Tsudik, Dan Massey, and Christos Papadopoulos. 2010. Named Data Networking (NDN) Project. *Technical Report NDN-0001, Xerox Palo Alto Research Center-PARC* (2010).

[163] Yu Zhang, Zhongda Xia, Spyridon Mastorakis, and Lixia Zhang. 2018. KITE: producer mobility support in named data networking. In *ACM Conference on Information-Centric Networking*. ACM, 125–136. https://doi.org/10.1145/3267955.3267959

[164] Zhiyi Zhang, Yingdi Yu, Alexander Afanasyev, Jeff Burke, and Lixia Zhang. 2017. NAC: Name-based access control in named data networking. In *ACM Conference on Information-Centric Networking*. ACM, 186–187. https://doi.org/10.1145/3125719.3132102

[165] Zhiyi Zhang, Yingdi Yu, Haitao Zhang, Eric Newberry, Spyridon Mastorakis, Yanbiao Li, Alexander Afanasyev, and Lixia Zhang. 2018. An overview of security support in Named Data Networking. *IEEE Communications Magazine* 56, 11 (2018), 62–68. https://doi.org/10.1109/MCOM.2018.1701147

[166] Qingji Zheng, Guoqiang Wang, Ravishankar Ravindran, and Aytac Azgin. 2015. Achieving secure and scalable data access control in information-centric networking. In *IEEE International Conference on Communications (ICC)*. IEEE, 5367–5373. https://doi.org/10.1109/ICC.2015.7249177

[167] Liehuang Zhu, Nassoro MR Lwamo, Kashif Sharif, Chang Xu, Xiaojiang Du, Mohsen Guizani, and Fan Li. 2020. T-CAM: Time-based content access control mechanism for ICN subscription systems. *Future Generation Computer Systems* 106 (2020), 607–621. https://doi.org/10.1016/j.future.2020.01.039