

Name privacy on named data networking: a survey and future research

Mohammad Shahrul Mohd Shah¹, Yu-Beng Leau², Mohammed Anbar³, Liang Zhao⁴

¹Faculty of Computing and Informatics, Universiti Malaysia Sabah, Kota Kinabalu, Malaysia

²Cybersecurity Research Lab, Faculty of Computing and Informatics, Universiti Malaysia Sabah, Kota Kinabalu, Malaysia

³National Advanced IPv6 Centre, Universiti Sains Malaysia, Gelugor, Malaysia

⁴School of Computer Science, Shenyang Aerospace University, Shenyang, China

Article Info

Article history:

Received May 5, 2024

Revised Jan 17, 2025

Accepted Mar 3, 2025

Keywords:

Information-centric networking

Name obfuscation

Name privacy

Named data networking

Survey paper

ABSTRACT

Information-centric networking (ICN) has gained significant interest in recent years, attracting both academic and industry, it represents a paradigm shift and moving away from the host-based IP networks that dominate today landscape. As ICN technology matures and advances towards real-world deployment, the importance of addressing security and privacy concerns has grown exponentially. The ICN paradigm is deliberately designed to encompass numerous security and privacy features, including but not limited to provenance and privacy. These features, which are often lacking in the host-centric paradigm, inherently form a core aspect of ICN. Nevertheless, due to its relatively recent emergence, the ICN paradigm also presents a range of unresolved privacy challenges. This paper offers a comprehensive survey of the existing literature on privacy primarily focuses on major domains name privacy. We delve into the fundamental principles of existing research and evaluate the limitations of proposed methodologies. In name privacy, we also explore strategies to preserve name privacy. We have identified future research directions and highlighted ongoing challenges in the pursuit of enhancing ICN privacy.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Yu-Beng Leau

Cybersecurity Research Lab, Faculty of Computing and Informatics, Universiti Malaysia Sabah

Kota Kinabalu, 88400, Malaysia

Email: lybeng@ums.edu.my

1. INTRODUCTION

As the internet has grown in popularity, use cases have extended beyond just the dissemination of multimedia content. TCP/IP, which stands for transmission control protocol over internet protocol, was developed with the main objective of improving the communication between computers within a network. Furthermore, online gaming and popular streaming services such as Netflix, YouTube, and Facebook contribute to rising number of IP traffic, with more than three times as many devices predicted to be linked to IP networks by year 2023. There will be 3.6 networked gadgets per person, up from 2.4 in 2018. The number of connected devices is expected to increase significantly from 18.4 billion in 2018 to 29.3 billion by 2023 [1].

TCP/IP, initially designed for user information exchange, is now exclusively utilized for content distribution. Alternative methods such as peer-to-peer (P2P) networks, distributed hash tables (DHT), and content delivery networks (CDN), have been developed to improve content distribution over the internet. However, these solutions are unsuitable due to packet transport delay caused by network infrastructure.

As the internet continues to evolve, new architectures have been developed to address various issues. Content-centric architectures have gained popularity and the National Science Foundation (NSF) has suggested information-centric networks (ICN) as a potential future internet design. Named data networking (NDN) is promising candidate for network architecture design, revolutionizing content sharing by assigning unique names to each piece of content. This simplifies content retrieval for users. Additionally, NDN addresses concerns like domain name system (DNS) overhead, user anonymity, and mobility through its naming system.

NDN content-centric approach has the potential to revolutionize the way we think about the Internet architecture and it remains as a promising candidate for future network design. NDN utilizes human readable hierarchical name that identifies the content and NDN users can get the content they want by utilizing this name. Naming components are separated by with the use of either forward slashes ('/') or periods ('.') and have a semantic relationship with a content.

Content names may disclose significant information through their routable and non-routable components. Routable components demonstrate characteristics that are equivalent of a combination of DNS names and IP addresses. They have the characteristic of being easily readable by user, similar to DNS names, and they fulfill a comparable function to IP addresses by directing routers to the subsequent destination for data interests.

In ICN-based architecture, privacy has always proven elusive. The native feature of NDN that exposes content names gives rise to concerns over the privacy of names. Name privacy refers to the level of public disclosure of content names in NDN, which has the potential to undermine user privacy. The hierarchical structure of the name in an Interest packet puts the contents at risk, establishing how important of preserving these names in order to ensure user privacy. The objective of reviewing existing name privacy approaches is to gain an in-depth knowledge of the processes, compromises, and effectiveness in maintaining the native features of NDN.

This survey article focuses on the most significant name privacy challenges in NDN. While NDN able mitigates many security issues associated with IP and introduces interesting novel security features, it also presents new challenges that must be considered. Some of these concerns can be resolved through existing solutions, while others require significant architectural changes. By drawing attention to these more complex challenges, we hope to encourage greater interest and spur further research efforts. Not only that, this survey paper also provides an in-depth exploration of the concept of name privacy within the context of NDN.

The rest of this paper is divided into four sections. In section 2, we reviewed through existing literature, finding a solution that preserve name privacy within the NDN architecture. We categorize these solutions into three techniques: name obfuscation, single-proxy-based methods, and proxy re-encryption. Each technique has its own unique strengths and potential weaknesses, by offering a comprehensive overview of these techniques, we aim to provide readers with an understanding of the different strategies used to preserve name privacy in NDN. Section 3, we described our review analysis and their research trend based on years. In this section also we described the challenges and open issues in terms of privacy in NDN. Finally, section 4 concludes the paper.

2. PROPOSED SOLUTIONS OF PRESERVATION OF NAME PRIVACY IN NDN

Incorporating name privacy into ICN-based infrastructures is not a straightforward process since it requires an upper-layer service to serve as a name prefix, which can be used to encrypt content or to segregate content ID and locator [2]. Preserving hierarchy in any form can lead to information loss and scalable routing cannot be accomplished without it. Integrating name privacy into ICN-based infrastructures requires balancing hierarchy and scalability while ensuring that the encryption process preserves content-sensitive information. In addressing this challenge, the countermeasure can be classified into three groups: content name obfuscation, proxy-based name obfuscation, and packet overlay.

2.1. Content name obfuscation

Name obfuscation is a technique employed to prevent eavesdroppers from identifying the person of interest [3]. However, message headers in NDN are not always confidential and security measures are limited to reply messages, despite the capability to secure application payloads [4]. Content names constitute a vital component of NDN forwarding structure, yet they can also disclose sensitive information such as the host's identity, the prefix indicating the type of application running on the host, and the delivered content. To tackle this challenge, countermeasures can be categorized into three distinct group: symmetric key based, full name homomorphic encryption, and bloom filter-based obfuscation.

2.1.1. Symmetric key based name encryption

Arianfar *et al.* [5] were the first to investigate the issue of preserving user anonymity. It involves producers blending sensitive content with 'cover content.' When consumers request this mixed content, their true request remains partially hidden. While this approach enhances storage and bandwidth capacity, it lacks protection against malicious producers and does not establish unlikability between consumers and producers. In work [6], the author proposed a content name privacy (CoNaP) scheme that ensures attackers cannot obtain content information from the content name. The author uses symmetric keys in allowing consumers to encrypt the name in the interest packet. CoNaP initiates a three-way handshake at the intermediate node (IN) to obtain the key and decrypt the true name of the content, allowing the consumer to verify the authenticity of the received interest packet.

This mechanism enables both the consumer and IN to verify each other's identity. Despite the proposed mechanism ability to preserve name privacy through encryption, increase latency and mobility challenges can be seen in Table 1. A mechanism that relies on name obfuscation to protect a user's privacy can create a conflict between users' expectation of efficient system performance and the need for obscured data that requires additional processing time to disclose the actual data. This conflict will result in a decrease in service-quality expectation, which directly leads to an efficiency loss due to name obfuscation.

Table 1. Summary of symmetric key based name encryption approaches

Ref.	Year	ICN model	Evaluation metrics	Strength	Weaknesses
Leshov <i>et al.</i> [6]	2019	NDN	a) Interest satisfaction delay (ISD)	Simulation showed proposed scheme has high ISR and less ISN compared to [7]	Signature privacy will be compromised
			b) Interest satisfaction ratio (ISR)	Support in-network caching compared to existing methods	Such security measures have an impact on latency and mobility

2.1.2. Full name homomorphic encryption

Another name obfuscation technique involves the full obfuscation of the content name through homomorphic encryption. Fotiou *et al.* [8] proposed an approach that involves a hierarchy of encrypted content brokers, where producers transmit an encrypted data to this hierarchy. The hierarchy then handles decryption, and consumers request content through brokers. Brokers respond with either references to child brokers or pointers to the original content producers. The technique utilizes additive homomorphic encryption to secure each query, enabling brokers to perform operations on them without requiring decryption.

There are two primary types of searchable encryption (SE), the most widely used ones are public key with keyword search (PEKS) and searchable encryption scheme (SSE). Incorporating searchable encryption technology, Jiang *et al.* [9] introduces a Group-based naming scheme. Author also delves into recent advancements in searchable and attribute-based encryption technologies, while addressing the challenges associated with their integration to ensure network privacy. Next, Ko *et al.* [10] presented a strategy called PEKS in NDN and have an objective to preserve the confidentiality of content names. This innovative approach draws on principles from route strategic planning and multicast, which were initially introduced in work [11].

Searchable encryption (SSE) empowers users to securely move data to the cloud by sending a secret and restricted query to the cloud service provider to ensure data privacy. The ciphertext is the sole piece of information that the server interacts with that conceals the plaintext details. The server single-handedly learns the ciphertext through this disguised query and nothing else about the plaintext. To further preserve name privacy, producers initially publish their public key in a one-way function known as a trapdoor to both consumers and routers before distributing their public key. Using the producer public key, consumers employ PEKS to encrypt specific Interest packets, while routers represent alternative encrypted Interest names by matching them with widely distributed trapdoor functions. However, this approach encounters limitations when encrypting longer names, resulting in increased content size, higher storage requirements, and extended execution times. In response, the authors work in [12] presents an improvement in the form of a Two-Tier design, wherein each router is allocated different trapdoor capacities. This enhancement aims to address and evaluate the performance challenges posed by the original mechanism.

In another work of homomorphic-based name obfuscation, the work presented in [13] introduces the privacy-aware transmission scheme in NDN (PATs NDN). This approach utilizes proxy re-encryption and blind algorithms to obscure content names. Similarly, in the work [14], a concept akin to name privacy preservation is explored, with different in cryptographic methods. Here, the author concentrates on protect named content by proposing hierarchical naming within sensory data centric named data networking

(SDC-NDN) and employs an elliptic curve-based name privacy protection mechanism. In Table 2, we summarize the approach that utilizes homomorphic based name obfuscation.

Table 2. Summary of full name homomorphic encryption

Ref.	Year	ICN model	Evaluation metrics	Strength	Weaknesses
Fotiou <i>et al.</i> [8]	2019	PURSUIT	a) Communication overhead b) Computational overhead	Proposed approach made for publish-subscribe paradigm but can be applied to content-centric networking (CCN) and others paradigm	Such security measures may have an impact on latency and mobility
Jiang <i>et al.</i> [9]	2015	NDN	a) System performance b) Retrieval time performance	Mapping human-readable hierarchical naming to integer grouping can prevents attackers from snooping the router and leaks routing information Able to mitigate snooping attack	- Proposed scheme may not run effectively in resource-constrained environments. - Caching ability will have an impact to proposed naming scheme
Guo <i>et al.</i> [13]	2018	NDN	a) Time for provider produces content packet b) Time for consumer extracts content from a content packet	Name privacy of content name is secured due to full name obfuscation	Multiple encryption/decryption process going on, result delay in data transfer
He <i>et al.</i> [14]	2019	NDN	a) Producers operation b) Requesters operation c) Latency	Caching longest name prefix matching is still remain preserved	Packet name encryption/decryption, will affect time performance, latency, and storage space
Ko <i>et al.</i> [10]	2020	NDN	a) Average download time b) Cache hit ratio at router	Without a master secret key to extract private keys, the suggested technique can preserve privacy better	- Searching names in network requires the PEKS algorithm to validate encrypted, reduces performance - Repeated process, high latency

2.1.3. Bloom filters based obfuscation

Maintaining name privacy in NDN can be achieved through the use of bloom filter, as highlighted by work [15]. In this approach, consumers construct a hierarchical bloom filter denoted as $HB = (B1, B2, \dots, Bn)$, where Bn represents the bloom filter for name components up to the n -th level. To illustrate, consider the filtering of content for $/ndn/pt/minho$. A consumer generates $B1$ for $/ndn$, $B2$ for $/ndn/pt$, and $B3$ for $/ndn/pt/minho$. Subsequently, a router checks its cache for the presence of Bn and responds to the consumer if it exists there. If Bn is not found in the cache, the router consults the pending interest table (PIT) for Bn . If Bn is present in the PIT, the corresponding PIT's bloom filter is updated by incrementing a counter, and the request is dropped, as it has already been forwarded. This method effectively obfuscates the name in the interest request, transforming it into a randomized bit string, thereby protecting user privacy. However, it is important to note that bloom filters may occasionally produce false positives in name matching.

Massawe *et al.* [16] proposed SP-NDN, a scalable and privacy-preserving routing protocol for NDN. They employed bloom filters to enhance keyword search efficiency while protecting original keywords. Addressing the name privacy attack, they introduced a content-dependent key tree-based multicast encryption scheme. Both consumer and producer will utilize bloom filters to store shared names and secret keys of Interest packets, verifying them before forwarding to prevent leakage. However, multiple bloom filters may lead to memory overhead. While employing bloom filters to preserve name privacy by concealing keywords in names, there are drawbacks to consider. Attackers can learn to represent names using bloom filters, potentially disabling the filters that hide suppressed names [17]. Additionally, for the bloom filter to function, consensus on the hash functions among producers, intermediate routers, and consumers is necessary. Using the same set of hash algorithms for all system names may increase the likelihood of false positives [18] which can be seen in Table 3.

Table 3. Summary of bloom filter-based obfuscation

Ref.	Year	ICN model	Evaluation metrics	Strength	Weaknesses
Massawe <i>et al.</i> [16]	2013	NDN	Probability of a false positive	With the use of multiple bloom filter, author able to reduce false positive probability	With multiple bloom filter usage, dynamic network environment will be a challenge

2.2. Single proxy-based name obfuscation

In this mechanism, the interaction between a user and the network system is simplified as the user only needs to engage with a single proxy. This proxy will serve a dual role, handling both the encryption of interest's packet and the decryption of content, streamlining the process and enhancing the user experience. Mechanism that utilized single proxy-based name obfuscation is lightweight coding techniques like random linear network coding or Huffman coding to address privacy, security, data integrity issues efficiently with low resource consumption. These methods are not resource-intensive, making them suitable for various applications. In these approaches, a single proxy handle tasks like interest and content encryption/decryption, simplifying user interaction. Therefore, we classify these methods into Network coding and Huffman coding subcategories.

2.2.1. Network coding-based approach

Network coding [19] is a contemporary domain within information theory that enables intermediate nodes to generate new packets by merging packets received from incoming edges. A straightforward illustration in a wireless context involves a six-node topology, as depicted in Figure 1. Node A and Node B serve as source nodes, with node A transmitting to E and F, and node B doing the same to E and F. Instead of transmitting separately, when network coding approach is used the two packets from the source are combined by means of XOR operations at the intermediate node C and forwarded.

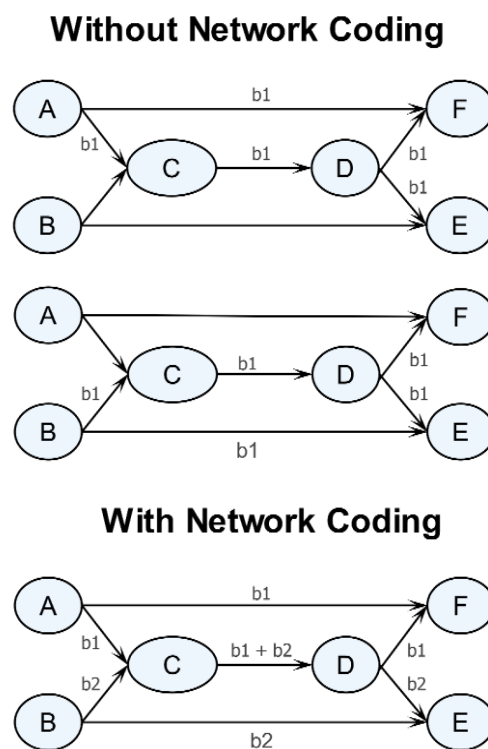


Figure 1. Process between with and without network coding

Linear network coding [20] is commonly employed to enhance network throughput. In this approach, network nodes linearly combine multiple packets for transmission, maximizing information flow, rather than merely relaying received packets. Random linear network coding [21] is a potent variant of linear network coding schemes. Author in the work [22] proposed network coding-based mutual anonymity communication protocol for NDN (NC-MANDN), Utilizes ICN's inherent content chunking along with random linear network coding (RLNC). To request content, the user divides the interest into smaller encrypted chunks using a trusted proxy public key. Once enough chunks are received, the proxy reconstructs the original interest packet and forwards it to the content provider. Similarly, the content provider breaks down the content into chunks and sends them to the proxy. However, this scheme raises concerns about underutilized caching and the high cost of asymmetric-key cryptographic operations which can be seen in Table 4.

Table 4. Summary of network coding-based name obfuscation

Ref.	Year	ICN model	Evaluation metrics	Strength	Weaknesses
Tao <i>et al.</i> [22]	2015	NDN	N/A	Use of a logical overlay network and random routing for forwarding can be effective in mitigating timing attacks	Limited cache utilization and high cost of asymmetric-key cryptographic operations

2.2.2. Huffman coding-based mitigation

Huffman coding is a lossless data compression algorithm that operates by assigning variable-length codes to input characters. The length of each assigned code is determined by the frequency of its corresponding character. Tourani *et al.* [23] addressed the subject of censorship in NDN by introducing a lightweight anticensorship framework founded on Huffman coding. This framework relies on a distinct Huffman encoding table that is shared among each user and a trusted proxy. In order that will mitigate name censorship, the user employs partial encoding of the content name, with particular emphasis on the suffix. The user initiates an interest by encoding content name components using Huffman coding and appending a predefined plaintext prefix like "/anonym." This interest, with the plaintext prefix "/anonym", is then routed to a specific node in the ICN network called an anonymizer, which functions similar to a Tor exit node. Anonymizer can only access the content name requested by the user and serves it from its Content Store (CS) if available, or requests it on the user behalf.

However, there are several drawbacks that arise from this approach. Initially, it necessitates extra communication overhead to reach the anonymizer before able to accessing any content, even if the content is cached along the path to the anonymizer. As a result, certain advantages of ICN, such as optimized in-network caching are lost. Furthermore, due to the uniqueness of the encoding table, NDN encounters a predicament in terms of content reusability. In conclusion, if the anonymizer is curiosity-driven, it can potentially deduce user interests by analyzing the connection between these interests and their respective authors through the established security association, as shown in the summary in Table 5.

Table 5. Summary of Huffman coding-based name obfuscation

Ref.	Year	ICN model	Evaluation metrics	Strength	Weaknesses
Tourani <i>et al.</i> [23]	2015	CCN	a) Average download time b) Protocol overhead c) Round trip time	Lightweight framework suitable for mobile user	Extra communication overhead to reach the anonymizer

2.3. Proxy re-encryption-based name obfuscation

The primary objectives of proxy re-encryption techniques is to protect both the content and the associated names from network nodes responsible for delivering content to its intended recipient [24]. Simply preserving the name privacy is not sufficient because attacker could mimic similar interests packet. Even with cryptographic protocols in place, the possibility of content being obfuscated with irrelevant data, making it challenging for intruders to discern genuine content from the noise. However, the primary challenge with randomization is that it can make it a challenge to recover the original content from the noisy version. Additionally, this process introduces substantial communication overhead [25].

Asghar *et al.* [26] introduced privacy-preserving information lookup in content-centric networks (PROTECTOR), aimed at securing names and content in CCN. Built on the foundation laid by Fotiou *et al.* [27], which utilizes proxy encryption, PROTECTOR ensures users and CCN nodes to not share keys with one another. To protect user interests, clients first translate content name components into matching trapdoors, which are then sent to CCN nodes for encrypted matching. Upon a successful match, CCN nodes act as proxies, pre-decrypting content before delivery to users, who must perform the final decryption. However, this mechanism faces scalability and key management challenges. Users need unique proxy re-encryption keys from a key manager upon startup, and computational complexity and storage/bandwidth linearly increase with the number of users, posing issues for large-scale deployment [28].

Authors also presented their implementation and evaluation studies in PrivICN [29], a scheme pre-serving user privacy in ICN through proxy-based encryption. This approach employs asymmetric encryption to preserve name privacy during content lookups and the message flow is still the same in ICN only author added step 1.4 and 6 in their proposed mechanism as seen in Figure 2. While effective, this method can introduce computational overhead. PrivICN represents an enhancement over the authors prior work, demonstrating their ongoing focus on preserving name privacy in ICN.

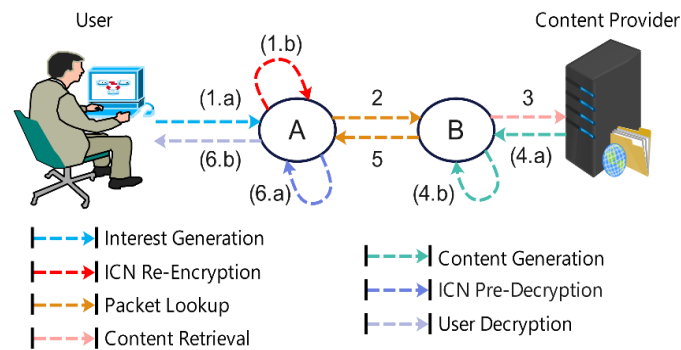


Figure 2. PrivICN Approach [29]

NDN enjoys a built-in advantage for user privacy due to the absence of source and destination network addresses. However, ICN architectures, where data names serve routing and search functions, introduce challenges. Retrieval names have semantic links to the content, potentially revealing user information if monitored by attackers [30]. Additionally, NDN's named content and advanced routers with ample memory and computational power can facilitate more straightforward and efficient Internet censorship [15]. The summary of proxy re-encryption technique can be found in Table 6.

Table 6. Summary of proxy re-encryption-based

Ref.	Year	ICN model	Evaluation metrics	Strength	Weaknesses
Ashgar <i>et al.</i> [26]	2019	NDN	a) Average lookup time in the FIB table (ms) b) FIB table size (Mb) c) Download time (ms.) d) Delay	The system prioritizes ease of user management, particularly in terms of adding and removing participants at a minimal cost	Proposed mechanism has the potential to introduce delays and computational overhead

2.3.1. Packet overlay

Deep packet inspection (DPI) [31], one of the most precise techniques for analyzing and categorizing internet traffic that is applied by internet service providers (ISP). However, due to the significant memory and processor demands, establishing high-performance DPI solutions necessitates careful consideration of computer system design. In contrast to IP networks, ICN is vulnerable to attackers' using DPI along the end-to-end communication channel to intercept unencrypted communication. DPI can also be used in ICN to determine content sensitivity. However, doing so can threatens user privacy [32].

Cui *et al.* [33], [34] proposed a scheme that is designed to counteract name-watchlist attacks and DPI through censorship techniques. Their primary goal is to develop an anti-censorship system capable of combatting Internet censorship while preserving privacy within the context of NDN. In their approach to circumventing censorship, author suggests disguising certain names as valid while preserving the censored name as the original name. This technique utilizes content stores, which cached data packets for future requests and allow intermediate routers to identify two names that refer to the same content.

In the event of an attack, the producer discovers that the requested name is censored, DPI is deployed on cached data packets to flag sensitive keywords as censored [35]. If an interest packet contains these sensitive parameters, the request is blocked. This approach, however, poses a challenge to the effectiveness of anticensorship measures when caching features is fully utilized. To address this issue, the author suggests the use of smart routers to enhance network flow. These smart routers play a crucial role in recovering the original name from the genuine name, thereby distinguishing between the two disguised names. We categorize packet overlay into onion routing and VPN based tunnelling.

a. Onion routing based tunnelling

The onion routing [36] involves the use of multiple layers of coordinated encryption and intermediary nodes tasked with progressively removing these layers as data packets traverse through the network. Anonymous named data networking application (ANDa⁻NA) [37] is an onion routing overlay network tailored for NDN, which offers heightened level of privacy and anonymity to end-users. ANDa⁻NA has been purposefully crafted for NDN with an onion routing approach, aiming to provide a level of consumer anonymity on par with Tor, the most prevalent system for achieving user anonymity within the IP domain. To achieve anonymity using onion routing, encapsulated packets traverse through circuits, each

composed of multiple willing hosts referred to as anonymizing routers, or simply onion routers [35], [38]. This complex network configuration is designed to obscure the origins of data packets.

ANDa⁻NA relies on a multi-layered, paired-centric encryption system and directs data from the consumer through a sequence of routers as shown in Figure 3, before data transmission, the user establishes an ephemeral circuit by selecting a pair of anonymizing routers (AR) and securely shares them with two symmetric keys used for encrypting the packets within the circuit. The router located closer to the users end is referred to as the entry (AR1) while the other is known as the exit (AR2). Each data packet undergoes a process of encapsulation within layers of encryption. The consumer encrypts their Interest packet using the public keys of the corresponding AR.

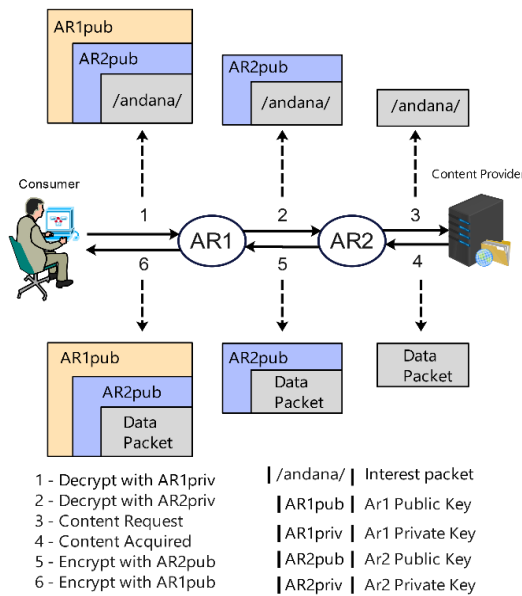


Figure 3. Dual proxies in ANDa⁻NA model [37]

On the return journey, the content packet is successively encrypted by each AR using the symmetric keys that were shared prior to the start of communication process [39]. Following this, advancements in ANDa⁻NA were introduced in the work by Tsudik *et al.* [40], which demonstrates the application of onion routing to achieve session anonymity within the NDN framework. The proposed mechanism employs two or more AR along the path between the consumer and the producer. However, once the name-spaces become encrypted to the point where only the requesting entities can decipher them, the practicality of the CS diminishes, rendering it ineffective for consumers to retrieve content.

Not only that, tunneling has the potential to degrade NDN performance, mainly because it neglects the possibility of in-network caching. The authors have advised that it should be reserved for situations involving privacy-sensitive content. Furthermore, Seo *et al.* [41] put forward a method that combines elements of Tor and a structure similar to ANDa⁻NA, employing a two-layered encryption approach in content-centric networking (CCN). While this approach is effective in countering censorship, it comes with certain drawbacks, including a substantial computational burden and increased delays at routers due to the repetitive encryption and decryption processes.

Additionally, routers encounter challenge of managing a large number of stored keys, which can overwhelm their storage capacity. Another variation of onion routing can be found in the work by in [42], where they embrace the approach outlined in [41] with some alteration. In this technique, public key encryption remains in use, but with an essential difference: the content name hash value is removed. Instead, a symmetric key is used to ensure content privacy, hence reducing the required number of encryption keys.

As work in [37] perform a routing in the network as anonymous nodes with the ability to have all nodes to sign the packet, which may compromise the signers identity. Ling *et al.* [35] proposed a mechanism for CCN privacy protection that also adopts hybrid encryption method that consists of combining group signature and encryption in hiding signer's real identities. Moreover, the proposed approach can take advantage of ubiquitous caching by implementing two layers of encryption. Author performed a comparison with the work in [37] and shows proposed mechanism only stored two symmetric keys as opposed to four

and this will resulting in lesser burden to routers. However, even with minimal computation and key storage overhead, it still in conceptual design without any actual implementation of it. Table 7 summarizes approach that utilize onion routing as packet overlay.

Table 7. Summary of onion-routing overlay

Ref.	Year	ICN model	Evaluation metrics	Strength	Weaknesses
Dibenedetto <i>et al.</i> [37] and Tsudik <i>et al.</i> [40]	2012	CCN	a) Round-trip time (RTT) b) Download time ratio	- Enable privacy and anonymity with cache-disabled configurations for perfect privacy - Mitigation for timing attacks	- Tunneling can reduce NDN performance since in-network caching is not feasible - Adds latency and computational overhead from repeated encryption/decryption, with limited applicability due to partial packet concealment - The high cost associated with performing multiple per-packet encryptions and decryptions
Seao <i>et al.</i> [41]	2017	CCN	Average throughput (Mbps)	The proposed approach is effectively resist local eavesdroppers	- Proposed solution did not effectively tackle the problem of covert communications in a contested environment - Lack security measures against compromised routers
Cui <i>et al.</i> [33], [34]	2019	NDN	Performance overhead: a) File receive ratio b) Average retrieval time	- Security analysis reveals the proposed system capable of defending against both name-watchlist attacks and deep packet inspections - Performance evaluation show that under conditions of low network traffic density, proposed scheme outperforms the original NDN scheme in file receive ratio and average file retrieval time	

b. VPN based tunnelling

Virtual private networks (VPN) further enhance name privacy within the NDN framework by establishing network tunnels for packet encapsulation. In work [43], authors aim to solve name privacy by designing NDN virtual private network. The design scheme encapsulates NDN inside NDN (NDN-in-NDN) which is the same as the traditional Internet architecture that utilize VPN (IP-in-IP). The proposed solution requires gateway as transparent proxy that are located on both side of consumer and producer. NDN-in-NDN retains the in-network caching benefits of NDN by using the same set of keys for encrypting and decrypting packets. However, a significant drawback of this mechanism is the vulnerability of the gateway; if an attacker gains control of the gateway, the entire network can be compromised.

Another anonymity solutions can be found in work CCVPN [7]. The proposed approach utilizes a gateway on the consumer side, where the producer encrypts packets using a symmetric key included in the Interest packet. Compared with the work in [43], caching within the domain is disabled and partial part of the packets name will be visible for forwarding process. As the hierarchical naming [44] feature can be exploited in terms of Data packets that cryptographically signed by content providers. Liu *et al.* [45] proposed an identity privacy protection strategy for vehicle named data network (VNDN) [46] that is based on ring signature scheme. Ring signatures are implemented to conceal any correlation that may exist between a signature and the source of the data. The proposed scheme also employs a single layer of anonymous proxy to conceal the content requester's true identity. Table 8 summarizes the VPN based approach.

Table 8. Summary of VPN-based name obfuscation

Ref.	Year	ICN model	Evaluation metrics	Strength	Weaknesses
Partridge <i>et al.</i> [43]	2017	NDN	N/A	The proposed mechanism retains in-network caching functionality	Gateway vulnerabilities cause network compromise if exploited Encryption and authentication to NDN network increase latency
Nunes <i>et al.</i> [7]	2017	CCN	a) Network throughput b) Request-response round-trip time (RTT)	Solid performance in network load capacity, even with added overhead from secure tunnel deployment	With the increasing number of consumers, it may lead to cryptographic overhead
Liu <i>et al.</i> [45]	2019	NDN	N/A	The privacy of both the user and the data provider's identities are protected	Complexity of the encryption /Decryption processes result in significant transmission delays

3. STATISTICAL ANALYSIS AND RESEACH CHALLENGES

In this section, we discuss the statistical analysis of recent research topics on NDN name privacy and their limitations. We examine the key techniques for existing name privacy approaches, categorize them based on their underlying mechanisms, highlight their strengths and weaknesses, and discuss common challenges faced by these approaches. Additionally, we aim to provide insights into potential research directions and contribute to more efficient name privacy solution in NDN.

3.1. Statistical analysis

ICN infrastructures fetch content by name that is semantically associated with it and makes data searching and retrieval are more efficient. Content names and their corresponding content are broadcast across the network in plaintext, so every ICN node that forwards the data can view it. A malicious ICN node could engage in censorship by blocking the delivery of specific content. As a result, securing the names and the contents of the ICN is crucial if one is to preserve the user privacy and reduce the likelihood of these potential threats.

More attention is need to be paid to the problem of name privacy in NDN, which has not been thoroughly investigated. Here, we present statistical charts to show the overview of recent research on technique to preserve name privacy, as shown in Figures 4(a) and 4(b). In Table 1 to 8, there is variety of different types of mitigation techniques used to preserve name privacy. Content name obfuscation in work [6], [8]–[10], [13]–[16], [47] single proxy-based name obfuscation in work [22], [23], [48], [49] proxy re-encryption based in work [26], [29], and tunnelling in [7], [33], [34], [37], [40]–[43], [45].

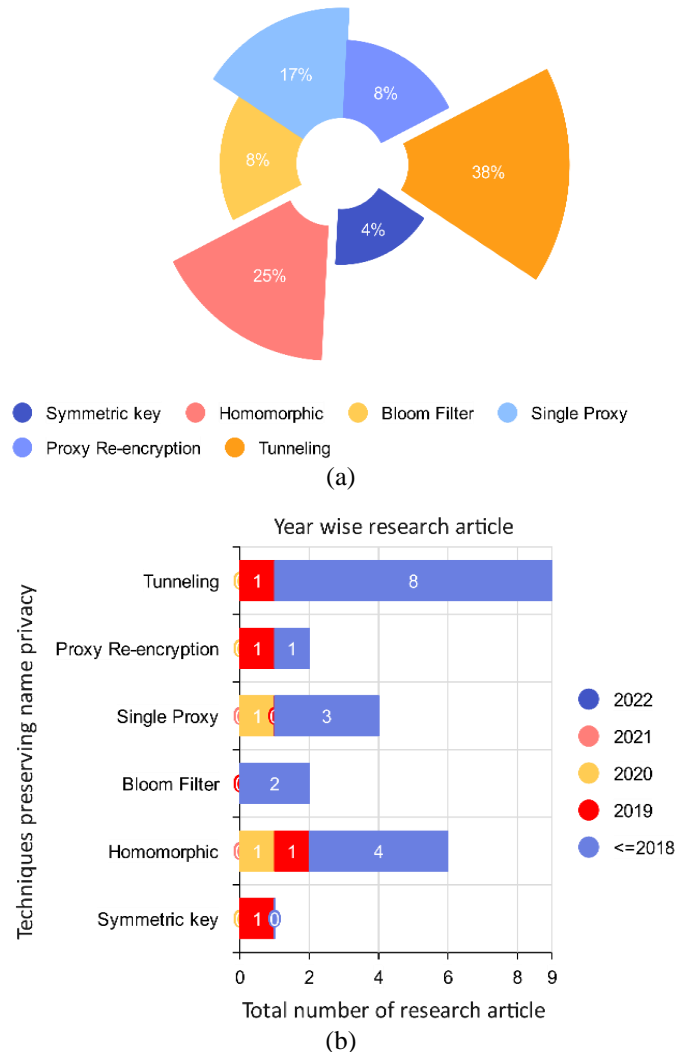


Figure 4. Statical analysis for timing attack (a) technique for mitigating timing attack and (b) year wise research article

In summary, we notice a trend towards enhancing name privacy by completely obfuscating the original name through the use of proxies for packet encapsulation. However, this approach comes with a cost, as it requires the reliance on trusted proxies, hence will increase the operational complexity and expenses. It is also important to keep in mind that current proxy solutions frequently overlook safety issues when recommending changes to data packet names, which could jeopardize integrity of the data [50]. Improving a naming scheme effectiveness and security is still an ongoing task. A thorough plan that addresses this must incorporate essential metadata that involves digital signatures, provider identities, and content hashes. In addition to secure naming, content providers certifying the manifest which contains hashes and chunk names that representing various option.

3.2. Open issue and research challenges

In this study, we have explored the current work in the domain of NDN name privacy. What we can summarize from this review is the negative impacts of suggested security measures or protocols on legitimate users can indeed be substantial, and it is crucial to examine the best strategies to alleviate these consequences. Many existing approaches introduce trade-offs between privacy, efficiency, and scalability, often resulting in increased computational overhead or reduced network performance. The adaptability of these solutions to dynamic network environments and real-world deployment remains a significant challenge.

DoS attacks can be mitigated by employing techniques such as rate limiting on suspicious interfaces and name prefixes, but this comes at the expense of a reduction in quality of service provided to legitimate users. Several privacy-focused schemes, such as those that use tunnelling or request labelling to avoid content caching, unknowingly affect user quality of experience and quality of service. For instance, user who is concerned about privacy could unintentionally label most of its content as private, rendering caching ineffective. This would contribute to increased network throughput.

Our analysis of various security vulnerabilities and potential attacks has led to the identification of several research issues that require further investigation in the context of NDNs. One of these issues is the development of a reliable mechanism for generating and verifying signatures in NDNs, which is a challenging task. Currently, NDNs use the SHA-256 algorithm for signature generation, but since signatures may need to be verified multiple times, the associated costs in terms of processing overhead, bandwidth, and verification time can be substantial. To mitigate these costs, it may be worthwhile exploring the possibility of developing an efficient batch signature verification system.

A significant area of research in NDNs is trust management between producers and consumers. Given the native feature of NDN architecture, user have the ability to assess whether a public-key owner is a suitable publisher for a particular piece of data prior to submitting a request. However, effective procedures are required for routers to trust a public key associated with a producer while verifying the content under the NDN methodology. This situation may require access to multiple public-key certificates for authentication purposes. Although researchers have developed hierarchical trust models to address this challenge, their complexity imposes a significant computational burden on the network. Therefore, it is crucial to establish an efficient trust model to manage this difficulty.

One of the most pressing research challenges in NDN is how to handle the privacy of names and content. Currently, data packets in NDN are signed by the content creator, but there is no standard encryption method to protect private content and data transmitted over the internet. Given that the names in NDN interest packets contain information about both the fetched material and the destination host, it is crucial to establish an encryption mechanism that can protect the content and data packet identity from potential interception or malicious attacks.

Performance gains come from using human-readable content names can help with efficient caching and interest aggregation. Nevertheless, this compromises user privacy. For example, in a country with strict censorship, users cannot access blocked content by its name because censors can filter these names. If content is cached before being blocked, censors can delete it from caches by name. Additionally, attackers have the capability to store and analyze user interests. Even those who prioritize privacy do not want their interests monitored by publishing content names without protection. Therefore, ensuring name privacy is a major challenge in NDN.

After conducting our analyses, we have concluded that the commercial adoption of NDN technology is uncertain. Original NDN concept has been enhanced through an application-driven, experimental research approach, resulting in significant progress. However, researchers have only scratched the surface of certain challenges, including security, trust models, scalable routing, data forwarding strategy design, and namespace structure. Several areas in NDN, such as lowering routing costs and protecting name and content privacy, require further research and development. The topics discussed in this article present opportunities for meaningful contributions to the field.

4. CONCLUSION

NDN is considered a leading candidate for ICN due to its content-based security, which is secure than the current TCP/IP model. On the other hand, NDN leaves itself open to the possibility of new kinds of attacks. This paper starts by outlining the most recent developments, approaches, applications, and gaps in research on privacy in NDN. First, we discussed the theoretical foundations of NDN and the technical approaches used to complete these objectives. Then we presented a complete summary of the scientific progress made in preserving name privacy. Finally, we address several issues and conduct statistical analysis for name privacy in NDN. Given the significance of characteristics, it is important that we preserve the privacy and overcome the vulnerabilities that it carried. Furthermore, open research issues are outlined, emphasizing the need for further exploration of NDN security and privacy by researchers in the field. Our future efforts will prioritize on securely preserving user privacy with minimal network overhead.

ACKNOWLEDGMENTS

We would like to express my sincere gratitude to University Malaysia Sabah (UMS) and the Faculty of Computing and Informatics for their invaluable support throughout this research. Their resources, guidance, and encouragement have played a crucial role in the completion of this work.

FUNDING INFORMATION

This research received no specific grant from any funding.

AUTHOR CONTRIBUTIONS STATEMENT

All authors contributed to this research in accordance with the Contributor Roles Taxonomy (CRediT). Contributions include conceptualization, methodology, formal analysis, and investigation. The corresponding author is responsible for overseeing the submission, revision, and publication process, ensuring communication among all authors.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Mohammad Shahrul Mohd Shah	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Yu-Beng Leau	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mohammed Anbar	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Liang Zhao	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study.

ETHICAL APPROVAL

This research does not involve human participants, personal data, or animal subjects; therefore, ethical approval was not applicable.

DATA AVAILABILITY

This study is in a form of survey paper that analyzes existing research on NDN name privacy. All information presented in this paper is derived from existing published studies, which are cited appropriately. Readers can refer to the cited sources for access to the original data and findings.




REFERENCES

- [1] Cisco “Cisco annual internet report (2018–2023) white paper,” Cisco, Accessed: May 5, 2024. [Online]. Available: <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html>
- [2] E. Ngai, B. Ohlman, G. Tsudik, E. Uzun, M. Wählisch, and C. A. Wood, “Can we make a cake and eat it too? a discussion of ICN security and privacy,” *ACM SIGCOMM Computer Communication Review*, vol. 47, no. 1, pp. 49–54, Jan. 2017, doi: 10.1145/3041027.3041034.
- [3] Z. Zhang, S. Y. Won, and L. Zhang, “Investigating the design space for name confidentiality in named data networking,” *Proceedings - IEEE Military Communications Conference MILCOM*, vol. 2021-Novem, pp. 570–576, 2021, doi: 10.1109/MILCOM52596.2021.9652892.
- [4] M. Baugher, B. Davie, A. Narayanan, and D. Oran, “Self-verifying names for read-only named data,” in *2012 Proceedings IEEE INFOCOM Workshops*, Mar. 2012, pp. 274–279, doi: 10.1109/INFOCOMW.2012.6193505.
- [5] S. Arianfar, T. Koponen, B. Raghavan, and S. Shenker, “On preserving privacy in content-oriented networks,” in *Proceedings of the ACM SIGCOMM workshop on Information-centric networking*, Aug. 2011, pp. 19–24, doi: 10.1145/2018584.2018589.
- [6] N. Leshov, M. A. Yaqub, M. T. R. Khan, S. Lee, and D. Kim, “Content name privacy in tactical named data networking,” in *2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN)*, Jul. 2019, pp. 570–572, doi: 10.1109/ICUFN.2019.8805919.
- [7] I. O. Nunes, G. Tsudik, and C. A. Wood, “Namespace tunnels in content-centric networks,” in *2017 IEEE 42nd Conference on Local Computer Networks (LCN)*, Oct. 2017, pp. 35–42, doi: 10.1109/LCN.2017.105.
- [8] N. Fotiou, D. Trossen, G. F. Marias, A. Kostopoulos, and G. C. Polyzos, “Enhancing information lookup privacy through homomorphic encryption,” *Security and Communication Networks*, vol. 7, no. 12, pp. 2804–2814, Dec. 2014, doi: 10.1002/sec.910.
- [9] X. Jiang and Q. Huang, “Efficiently preserving the privacy of the semantic routing in named data network,” in *Proceedings - 2015 IEEE 12th International Conference on Ubiquitous Intelligence and Computing, 2015 IEEE 12th International Conference on Advanced and Trusted Computing, 2015 IEEE 15th International Conference on Scalable Computing and Communications*, 20, 2016, pp. 686–689, doi: 10.1109/UIC-ATC-ScalCom-CBDCCom-IoP.2015.138.
- [10] K. T. Ko, H. H. Hlaing, and M. Mambo, “A PEKS-based NDN strategy for name privacy,” *Future Internet*, vol. 12, no. 8, p. 130, Jul. 2020, doi: 10.3390/fi12080130.
- [11] A. Afanasyev *et al.*, “NFD developer’s guide,” *NDN, Technical Report NDN-0021*, 2021.
- [12] K. T. Ko and M. Mambo, “Trapdoor assignment of PEKS-based NDN strategy in two-tier networks,” in *Proceedings - 2020 16th International Conference on Mobility, Sensing and Networking, MSN 2020*, 2020, pp. 607–613, doi: 10.1109/MSN50589.2020.00099.
- [13] X. Guo, C. Chen, M. J. Zhang, A. Ngaboyindekwe, and L. C. Cao, “Privacy-aware transmission scheme based on homomorphic proxy re-encryption for NDN,” *International Journal of Security and Networks*, vol. 13, no. 1, pp. 58–70, 2018, doi: 10.1504/IJSN.2018.090646.
- [14] H. He and B. Chen, “An elliptic curve based name privacy protection mechanism for sensory data centric named data networking,” in *Proceedings - 2019 15th International Conference on Mobile Ad-Hoc and Sensor Networks, MSN 2019*, 2019, pp. 56–62, doi: 10.1109/MSN48538.2019.00024.
- [15] A. Chaabane, E. De Cristofaro, M.-A. Kaafar, and E. Uzun, “Privacy in content-oriented networking: threats and countermeasures,” *ACM SIGCOMM Computer Communication Review*, 2012.
- [16] E. A. Massawe, S. Du, and H. Zhu, “A scalable and privacy-preserving named data networking architecture based on bloom filters,” in *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops*, Jul. 2013, pp. 22–26, doi: 10.1109/ICDCSW.2013.32.
- [17] D. Kondo, V. Vassiliades, T. Silverston, H. Tode, and T. Asami, “The named data networking flow filter: towards improved security over information leakage attacks,” *Computer Networks*, vol. 173, 2020, doi: 10.1016/j.comnet.2020.107187.
- [18] V. G. Vassilakis, L. Wang, L. Carrea, I. D. Moscholios, and M. D. Logothetis, “Scalable bloom-filter based content dissemination in community networks using information centric principles,” 2016.
- [19] J. Wang, J. Ren, K. Lu, J. Wang, S. Liu, and C. Westphal, “An optimal Cache management framework for information-centric networks with network coding,” in *2014 IFIP Networking Conference, IFIP Networking 2014*, 2014, pp. 1–9, doi: 10.1109/IFIPNetworking.2014.6857127.
- [20] S. Y. R. Li, R. W. Yeung, and N. Cai, “Linear network coding,” *IEEE Transactions on Information Theory*, vol. 49, no. 2, pp. 371–381, 2003, doi: 10.1109/TIT.2002.807285.
- [21] D. Wu, Z. Xu, B. Chen, Y. Zhang, and Z. Han, “Enforcing access control in information-centric edge networking,” *IEEE Transactions on Communications*, vol. 69, no. 1, pp. 353–364, 2021, doi: 10.1109/TCOMM.2020.3026380.
- [22] T. Feng, F. Xing, Y. Lu, and J. L. Fang, “Secure network coding-based named data network mutual anonymity communication protocol,” in *Proceedings of the 2015 International Conference on Electrical, Computer Engineering and Electronics*, 2015, vol. 24, pp. 1107–1114, doi: 10.2991/icecee-15.2015.209.
- [23] R. Tourani, S. Misra, J. Klierer, S. Ortegell, and T. Mick, “Catch me if you can: a practical framework to evade censorship in information-centric networks,” in *ICN 2015 - Proceedings of the 2nd International Conference on Information-Centric Networking*, 2015, pp. 167–176, doi: 10.1145/2810156.2810171.
- [24] S. Badsha, I. Khalil, X. Yi, and M. Atiquzzaman, “Designing privacy-preserving protocols for content sharing and aggregation in content centric networking,” *IEEE Access*, vol. 6, pp. 42119–42130, 2018.
- [25] X. Zhao and H. Li, “Privacy preserving data-sharing scheme in content-centric networks against collusion name guessing attacks,” *IEEE Access*, vol. 5, pp. 23182–23189, 2017, doi: 10.1109/ACCESS.2017.2740623.
- [26] M. R. Asghar, C. Bernardini, and B. Crispo, “PROTECTOR: privacy-preserving information lookup in content-centric networks,” in *2016 IEEE International Conference on Communications (ICC)*, 2016, pp. 1–7, doi: 10.1109/ICC.2016.7511193.
- [27] N. Fotiou, S. Arianfar, M. Särelä, and G. C. Polyzos, “A framework for privacy analysis of ICN architectures,” in *Privacy Technologies and Policy: Second Annual Privacy Forum, APF 2014, Athens, Greece, Proceedings 2*, 2014, pp. 117–132.
- [28] S. Al Azad, M. W., Tourani, R., Mtibaa, A., & Mastorakis, “Harpocrates: anonymous data publication in named data networking,” in *Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies*, 2022, pp. 79–90.
- [29] C. Bernardini, S. Marchal, M. R. Asghar, and B. Crispo, “PrivICN: privacy-preserving content retrieval in information-centric networking,” *Computer Networks*, pp. 13–28, 2019, doi: 10.1016/j.comnet.2018.11.012.
- [30] D. Qu, G. Lv, S. Qu, H. Shen, Y. Yang, and Z. Heng, “An effective and lightweight countermeasure scheme to multiple network attacks in NDN,” *IEEE/ACM Transactions On Networking*, vol. 30, no. 2, pp. 515–528, 2021, doi: 10.1109/TNET.2021.3121001.
- [31] M. Al-hisnawi and M. Ahmadi, “Deep packet inspection using Cuckoo filter,” in *2017 Annual Conference on New Trends in Information and Communications Technology Applications (NTICT)*, Mar. 2017, pp. 197–202, doi: 10.1109/NTICT.2017.7976111.
- [32] Y. Yoshinaka, K. Kita, J. Takemasa, Y. Koizumi, and T. Hasegawa, “Programmable name obfuscation framework for controlling




- privacy and performance on CCN,” *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, pp. 2460–2474, Sep. 2023, doi: 10.1109/TNSM.2023.3275250.
- [33] X. Cui, L. C. K. Hui, S. M. Yiu, and Y. H. Tsang, “Study of censorship in named data networking,” *Lecture Notes in Electrical Engineering*, vol. 354, pp. 145–152, 2016, doi: 10.1007/978-3-662-47895-0_18.
- [34] X. Cui, Y. H. Tsang, L. C. K. Hui, S. M. Yiu, and B. Luo, “Defend against internet censorship in named data networking,” in *2016 18th International Conference on Advanced Communication Technology (ICACT)*, Jan. 2016, pp. 1–1, doi: 10.1109/ICACT.2016.7423367.
- [35] J. Ling, W. Zhao, and Y. Gong, “A privacy preserving strategy based on anonymous group in content centric network,” *DEStech Transactions on Computer Science and Engineering*, no. aiea, 2017, doi: 10.12783/dtcse/aiea2017/15007.
- [36] D. Goldschlag, M. Reed, and P. Syverson, “Onion routing,” *Communications of the ACM*, vol. 42, no. 2, pp. 39–41, Feb. 1999, doi: 10.1145/293411.293443.
- [37] S. DiBenedetto, P. Gasti, G. Tsudik, and E. Uzun, “ANDaNA: anonymous named data networking application,” *arXiv:1112.2205*, 2012.
- [38] K. Kita, Y. Koizumi, T. Hasegawa, O. Ascigil, and I. Psaras, “Producer anonymity based on onion routing in named data networking,” *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 2420–2436, Jun. 2021, doi: 10.1109/TNSM.2020.3019052.
- [39] C. I. Fan, A. Karati, and P. S. Yang, “Reliable file transfer protocol with producer anonymity for named data networking,” *Journal of Information Security and Applications*, vol. 59, 2021, doi: 10.1016/j.jisa.2021.102851.
- [40] G. Tsudik, E. Uzun, and C. A. Wood, “AC3N: anonymous communication in content-centric networking,” in *2016 13th IEEE Annual Consumer Communications and Networking Conference*, 2016, pp. 988–991, doi: 10.1109/CCNC.2016.7444924.
- [41] S. C. Seo, T. Kim, and M. W. Jang, “A privacy-preserving approach in content centric,” in *2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*, Jan. 2014, pp. 866–871, doi: 10.1109/CCNC.2014.6994394.
- [42] Y. Kim, I. J. Kim, and C. Shim, “A strategy for preserving privacy in the CCN,” in *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, Oct. 2018, pp. 797–800, doi: 10.1109/ICTC.2018.8539428.
- [43] C. Partridge, S. Nelson, and D. Kong, “Realizing a virtual private network using named data networking,” in *ICN 2017 - Proceedings of the 4th ACM Conference on Information Centric Networking*, 2017, pp. 156–162, doi: 10.1145/3125719.3125720.
- [44] M. S. M. Shah, Y.-B. Leau, Z. Yan, and M. Anbar, “Hierarchical naming scheme in named data networking for internet of things: a review and future security challenges,” *IEEE Access*, vol. 10, pp. 19958–19970, 2022, doi: 10.1109/ACCESS.2022.3151864.
- [45] X. Liu, Q. Bing, X. Lu, L. Zhong, D. Wei, and G. Qu, “An identity privacy protection strategy in vehicle named data network,” in *2019 IEEE International Conferences on Ubiquitous Computing & Communications (IUCC) and Data Science and Computational Intelligence (DSCI) and Smart Computing, Networking and Services (SmartCNS)*, Oct. 2019, pp. 818–822, doi: 10.1109/IUCC/DSCI/SmartCNS.2019.00166.
- [46] E. T. da Silva, A. L. D. Costa, and J. M. H. de Macedo, “On the realization of VANET using named data networking: On improvement of VANET using NDN-based routing, caching, and security,” *International Journal of Communication Systems*, vol. 35, no. 18, 2022.
- [47] A. Elabidi, G. Ben Ayed, S. M. Gammar, and F. Kamoun, “Towards hiding federated digital identity: stop-dissemination mechanism in content-centric networking,” in *SIN ’11: Proceedings of the 4th International Conference on Security of Information and Networks*, 2011, doi: 10.1145/2070425.2070468.
- [48] “A consumer-driven access control approach to censorship circumvention in content-centric networking,” in *Proceedings of the 3rd ACM Conference on Information-Centric Networking*, 2016, pp. 186–194, doi: 10.1145/2984356.2984360.
- [49] Y. Zhu, Y. Tao, and R. Huang, “BEAcM-DP: a broadcast encryption anti-censorship mechanism based on directory proxy,” *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 2, 2020.
- [50] M. S. M. Shah, Y.-B. Leau, M. Anbar, and A. A. Bin-Salem, “Security and integrity attacks in named data networking: a survey,” *IEEE Access*, vol. 11, pp. 7984–8004, 2023, doi: 10.1109/ACCESS.2023.3238732.

BIOGRAPHIES OF AUTHORS






Mohammad Shahrul Mohd Shah    received his bachelor of computer science (B.Cs.) in Network Engineering from Universiti Malaysia Sabah in Malaysia in 2017. He received his Master of Computer Science (M.C.S) in Software Development from Universiti Malaysia Sabah in 2019. From 2019 he has joined the Faculty of Computing and Informatics at Universiti Malaysia Sabah to pursue his Doctor of Philosophy (Ph.D.) in Computer Science. In the meantime, he has joined the Department of Faculty of Computing and Informatics, Universiti Malaysia Sabah, as a research assistant, and his current research interests include named data networking, internet of things, and networking. He can be contacted at email: mohd_shahrulshah@yahoo.com.






Yu-Beng Leau    received his B.Sc. (Multimedia Technology) degree from Universiti Malaysia Sabah, an M.Sc (Information Security) degree from Universiti Teknologi Malaysia, and a Ph.D. (Internet Infrastructures Security) degree from University Sains Malaysia. He currently serves as a senior lecturer in computer science at Malaysia's Universiti Malaysia Sabah's Faculty of Computing and Informatics. His current research interests include intrusion detection and prediction, network security situation awareness, IPv6 security, the internet of things (IoT), and information centric networks (ICN). He can be contacted at email: lybeng@ums.edu.my.



Mohammed Anbar    received his bachelor's degree in computer system engineering from Al-Azhar University, Palestine, the M.Sc. degree in information technology from Universiti Utara Malaysia, Malaysia (UUM), and the Ph.D. degree in advanced Internet security and monitoring from University Sains Malaysia (USM). He currently serves as a senior lecturer with the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His research interests are malware detection, web security, intrusion detection systems (IDS), intrusion prevention systems (IPS), network monitoring, the internet of things (IoT), and IPv6 security. He can be contacted at email: anbar@usm.my.



Liang Zhao    received his Ph.D. degree from the School of Computing at Edinburgh Napier University in 2011. Before joining Shenyang Aerospace University, he worked as associate senior researcher in Hitachi (China) research and development corporation from 2012 to 2014. His research interests include ITS, VANET, WMN and SDN. He has published more than 120 papers. He served as the Chair of several international conferences and workshops, including 2022 IEEE Big-DataSE (Steering Co-Chair), 2021 IEEE TrustCom (Program Co-Chair), 2019 IEEE IUCC (Program Co-Chair), and 2018-2021 NGDN workshop (founder). He is Associate Editor of Frontiers in Communications and Networking and Journal of Circuits Systems and Computers. He is/has been a guest editor of IEEE Transactions on Network Science and Engineering, Springer Journal of Computing. He was the recipient of the best/outstanding paper awards at 2015 IEEE IUCC, 2020 IEEE ISPA, and 2013 ACM MoMM. He can be contacted at email: lzhaosau@sau.edu.cn.