Understanding Security and Privacy Characteristics of Hybrid-based IP-ICN Coexistence Architectures

Shruti Arora Chhagan Lal Mauro Conti

June 2021

Abstract

Information-centric Networking (ICN) is the revolution of the internet due to its many benefit over the current internet infrastructure, namely caching, location-independent routing, and data-centric security. ICN ensures seamless data transfer due to its content-centric nature. Due to its content-centric nature, it is a must to ensure that security and privacy are in place before a shift to ICN takes place. There are three ways to make a shift to ICN: 1) Underlay, deploying ICN under the IP; 2) Overlay, deploying ICN over IP; 3) Hybrid, deploying ICN with IP. In this paper, we center on hybrid ICN architectures, two architectures are analyzed to examine their security and privacy features. The two architectures discussed are Hybrid Information-Centric Networking (hICN), and Content Centric Inter-Networking (CONET). Background and related works, on ICN as a whole, and the two architectures are given, followed by the analysis of the two. Features namely Availability, Access Control, Non-repudiation, Integrity, and Authentication are studied under security. Whereas in privacy, Anonymity, Confidentiality, and Unlinkability are studied. The paper presents the implementation and the relevance of these features to ICN architecture. After analyzing these traits separately in the two architectures, a comparison is drawn between them. Lastly, the conclusions are formed with a discussion of future works.

1 Introduction

The World Wide Web is expanding at an exponential rate and is more accessible than ever before. It has revolutionized our daily lives, especially during the COVID-19 pandemic, bringing different parts of the world together. This fast-paced development of the World Wide Web calls for a change in the way we access it. The current Internet Protocols (IP) were written in the late 19th century, and ever since, the Internet itself has seen a drastic change and expansion[1]. However, the internet protocols have seen from very little to slow development [1]. The current internet protocols, which are IPv4 and IPv6, serve well. Nevertheless, in the past few years, internet architectures have undergone quite a few developments. One of them being Information-Centric Networking (ICN) architecture, that compared to the present TCP/IP architecture offers faster content delivery and more secure transfer of information [2].

The concept of ICN was formulated with security and privacy issues faced by TCP/IP architectures in mind [2]. There are a lot of ICN architectures presently under development or ready to be deployed [3, 4, 5]. The deployment process is a slow one, as the whole internet architecture cannot be turned overnight. Several parameters have to be taken into consideration before deploying any of the ICN architectures available. These parameters could include updating software, changing hardware, rewriting IP request structure, etc [6]. These variables are dependent on how a specific architecture is envisioned to work. Bringing these changes to every device is difficult. Hence, most of the deployments are small-scale and then increased further depending upon the feedback from the small test area [6, 7]. There are three deployment strategies: overlay, underlay, and hybrid [6]. Descriptions of these strategies are present in the next section. This research paper focuses on hybrid ICN architectures. Hybrid architectures try to employ the present TCP/IP protocols with the ICN ones, with minimal changes in the current internet architecture [5].

In any internet architecture the security and privacy (S&P) of the users are an integral part of any internet architecture [8]. Hence, making it a central theme for this paper.

The aim of this research paper is to:
Investigate the presence and implementation of security and privacy features in different hybrid-based ICN/IP coexistence architectures.
In an effort to study the security and privacy features, an examination of basic ICN features was carried out namely forwarding, routing, caching, and data-centric security model. The knowledge gained was necessary to understand the presence and absence of S&P features investigated in this paper. Given the scope of the research, two hybrid architectures were chosen: Hybrid Information-Centric Networking and Content Centric Inter-Networking. Both the architectures have been deployed on a large scale, making them the most efficient candidates for this research [9, 10]. The description of these architectures is presented in the following section.

This paper gives an in-detail report about the research conducted, results obtained, and the conclusions drawn at the end. The following section, gives the background knowledge about the ICN architectures and a brief description of architectures considered in this report. Section 3 presents the methodology followed to complete the research. Furthermore, section 4 discusses the parameters for analyzing the architectures, followed by their analysis in section 5. A discussion about the results obtained and conclusions drawn can be found in sections 6 and 7, respectively.

2 Background and Related Works

Before proceeding any further on investigating architectures, it is important to understand ICN architectures and the terms related to them. This section aims at giving a thorough but brief background knowledge to the reader about ICN. The first subsection gives a description of ICN, followed by deployment strategies. Lastly, the two architectures studied for the research are introduced.

2.1 What is Information Centric Networking

Current internet architecture is host-centric networking, implying that data transfer takes place from a server to the rest of the users in a network [11]. ICN allows for 'information', 'content' or 'data' centric networking as opposed to the traditional host-centric networking [12]. This approach removes the dependence on the security of transferring channels, instead centers on securing the content. This feature paves the way for another important characteristic of ICN that is caching, as the security of the data fetched is not dependent on its location anymore.

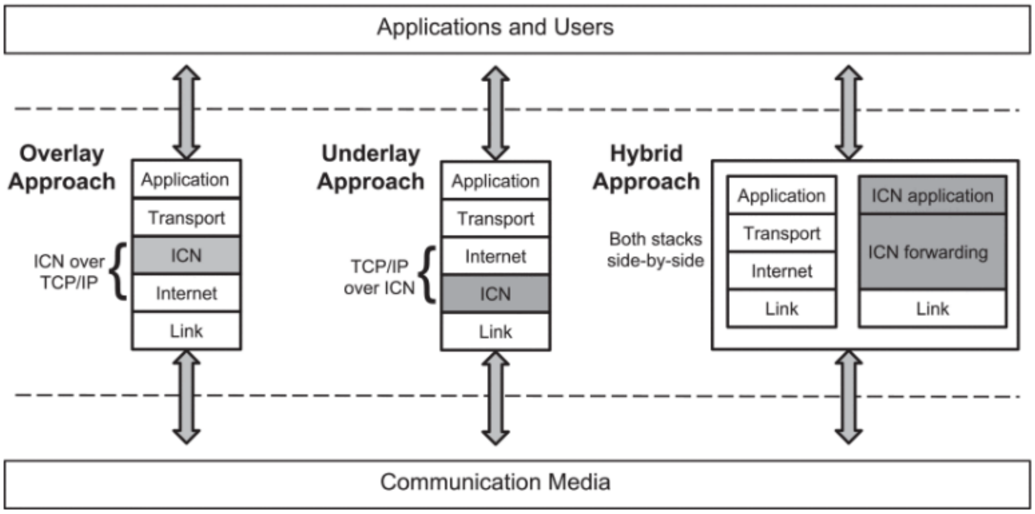

Figure 1: ICN Deployment Strategies: Overlay, Underlay and Hybrid [5]

*Caching*allows the intermediate routers to store a copy of data, further allowing for speedy retrieval of the same content if requested again. Due to caching, data retrieval requests in ICN architectures do not have to be fulfilled by the producer of the contents. One may even fetch data from a neighboring user in a cafe [13].
Every data request passes to nearby routers or devices that either send back the requested content or forward the request to their neighbors. This transfer of requests is called *forwarding*. Whenever the requested content is found, it is sent backward on the same path to the requester [11].
As data can be retrieved from any compatible device or router, be it the official producer or not, highlights the importance of anonymity. Hence, routing is based on content name rather than its location of content, making it IP independent. ICN architectures employ unique *naming* conventions to differentiate between data [11].

2.2 Deployment Strategies of ICN

There are three deployment strategies for ICN, based on the description in [5, 6], namely underlay, overlay and hybrid. The different deployment strategies are shown in figure 1.

Overlay can be seen as a deployment on top of current IP networks, usually described as *tunneling* approach. Moreover it allows for fast and easy deployment, making it a great option for ICN experimentation and testing [6].

Underlay is deploying ICN by modifying or adding application layer gateways. This kind of deployment usually allows for ICN routing inside the ICN network and requires a conversion gateway or proxies to connect to the rest of the internet [6].

Hybrid allows for deploying ICN with the current IP networks with minimal changes to the present hardware/software or internet infrastructure. This approach usually aims at making IP content aware and allowing for ICN semantics to be processed without compromising the processing of the current IP requests [6].

2.3 Hybrid Information Centric Networking Approaches

Given the scope of this research, only two of the hybrid approaches were considered, namely Hybrid Information-Centric Networking (hICN) and Content Centric Inter-Networking (CONET). Further paragraphs give details of these architectures.

2.3.1 Overview of hICN

hICN design allows using the current infrastructure of IP Networks to pass ICN requests or data packets integrated into IP packets. This design allows for a seamless processing of hICN packets as well as standard IP packets.

hICN eases the deployment of ICN with IPv4 and IPv6 by making IP packets content-aware [14, 15]. This paper considers the deployment of hICN with IPv6, the architecture presented in [16]. ICN request/reply protocols are inherited by hICN, in form of interest packets and data packets. Interest packets are for requesting data, whereas data packets are for forwarding requested data. These packets are made from regular IPv6 and TCP headers with modified fields, which provides differentiation from the standard IP packets. Data names are used instead of the IP address of the source or destination to provide name-based routing. For further details on hICN interest packets and data packets refer to [17]. As the standard IP packets are used, routers are tweaked to differentiate between hICN packets and regular IP-based packets based on their header fields. The hardware and software of the current routers are manipulated to allow ICN semantics. Usually, for name-based routing Forward Information Base (FIB) is required, and for hICN regular IP FIB is used. IP FIB is populated with IP addresses as well as hICN names using regular IP routing protocols. In order to provide caching, the memory buffers of IP routers are exploited to form a Pending Intrest Table (PIT) and Content Store (CS). PIT is to keep track of pending requests, whereas CS is used to store cache data. Figure 2 represents the working of FIB, PIT, and CS for routers enabled with hICN semantics.

Currently, CISCO is actively researching and developing hICN as it is an exceptional companion to 5G [10]. The testing of hICN has moved further from the controlled test-bed and is openly available for use at FD.io [14]. It is an open-source project under the Linux Foundation for the ICN community to test and experiment [15]. The aim is to provide support for the internet as mobile video, 5G, and IoT.

2.3.2 Overview of CONET

This paper discusses the hybrid approach of CONET, however, there is an overlay approach as well [18]. CONET, like hICN, discussed in the previous section, aims at bringing ICN features with minimal changes to the current internet paradigm. Like hICN, this architecture works with the standard IP requests but modifying them to be content-aware.

CONET is a network of several CONET Sub Systems (CSS) interconnected with end nodes and serving nodes [19, 18]. Each CSS is composed of border-nodes (BNs), end-nodes (ENs), serving-nodes (SNs), and optional internal nodes (INs). In a CONET, nodes exchange CONET Information Units (CIUs). CIU can be 'interest CIU' or 'named-data CIU', where

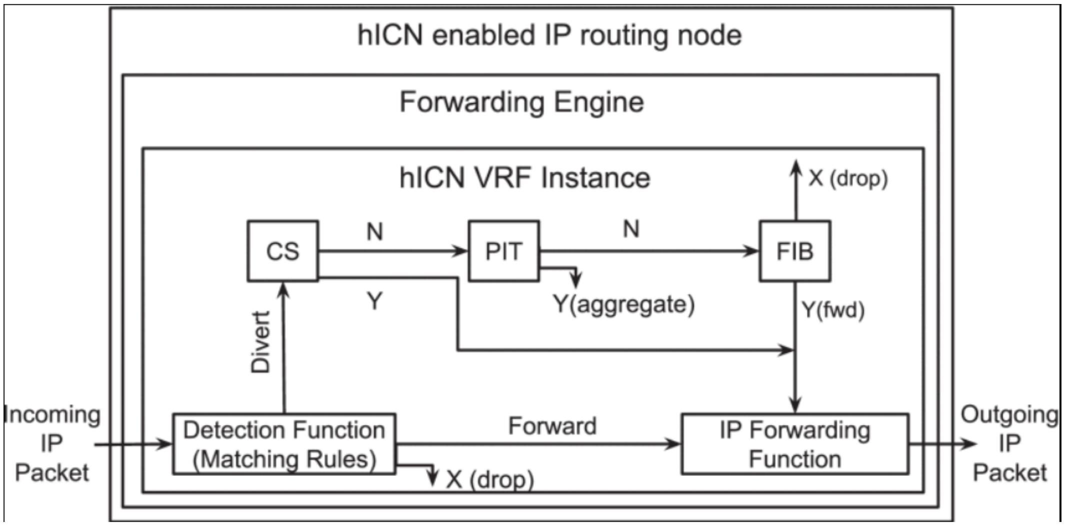

Figure 2: IP routers with hICN semantics [5]

interest CIU, requests for data, and named-data CIU carry named-data. Both CIUs, are referred to as carrier packets. End nodes are the devices that generate a request for named-data, that is interest CIU. Serving nodes send the named-data CIU after an interest CIU is received, and they are also responsible for storing cached data. Border nodes, as the name suggests, can be seen as entry gates to a CSS. These nodes are responsible for forwarding carrier packets to the next node in the CSS they are located or forward it to a BN of another CSS. Figure 3, represents the connection between 3 CSSs and their different nodes. CONET was devised and developed most during the CONVERGENCE project [9]. This network was used as the basis for implementing another ICN network called OFELIA [20]. CONET was deployed on top of the OpenFlow to form OFELIA.

2.3.3 Related Hybrid Approaches

This paper talks about two approaches, but it is worthwhile noting similar approaches for deploying ICN exists. One such is architecture is Content Labeling in IPv6 (CLIP), that like hICN exploits present IPsec [3]. However, CLIP inherits only caching and naming from the ICN characteristics and does not allow for stateful forwarding. Another approach to enable ICN with IP protocol is by using Network Function Virtualization (NFV) as a service (NFVaaS) [21]. This approach aims at dividing a network into two parts, that is ICN and IP, furthermore allowing virtual control functions to enable efficient content retrieval. Allowing both network protocols to exist in different regions.

3 Methodology

Having discussed the ICN features, and hybrid architectures, hICN and CONET in the previous section, this section gives an insight into how the research was conducted.

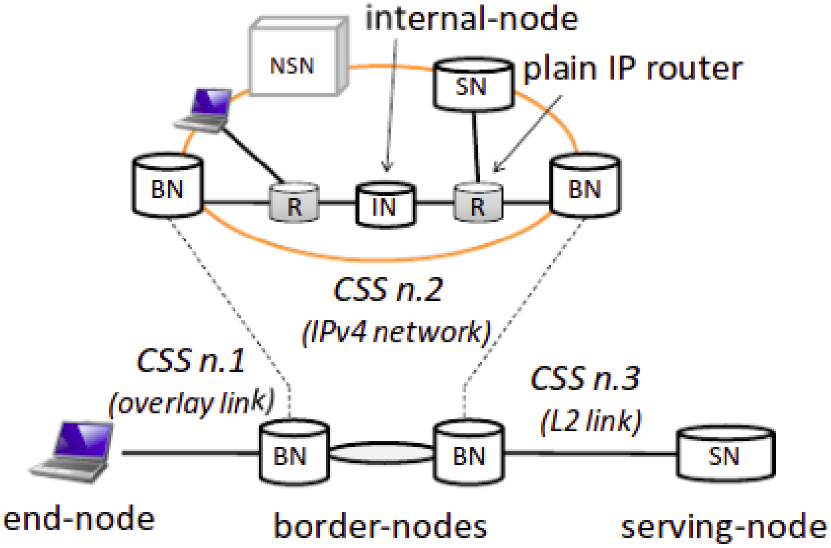

Figure 3: CONET architecture [18]

Steps followed for the research This research focused on presenting the privacy and security features of network architectures with the coexistence of IP and ICN in a hybrid approach. Given the scale of this research, two hybrid architectures were studied, namely:

- CONET
- hICN

In order to investigate the privacy and security features, it was crucial to gain an understanding of these architectures. Essentially, focusing on the implementation of original ICN features, which are discussed in detail in the next section. A thorough understanding of these architectures' implementation was obtained before drawing any results.

Material for the study A thorough literature study was performed over scientific material, peer-reviewed by the scientific community. In order to gather material, *Databases* Elsevier, ScienceDirect, IEEE Xplore, IETF Datatracker, and ACM were used. Materials presenting the most recent architectural information were used, as the analysis was based on several elements of IoT (Internet of Things), which are constantly developing.

Keywords used Information-centric networking, Content-centric networking, CONET, hybrid ICN

4 Analysis of Hybrid Architectures

This section presents the peculiarities that were investigated in the chosen architectures and their relevance to ICN architecture. First, the features that were studied are given in subsection 4.1, which include general ICN characteristics and S&P features, followed by their investigation in the two chosen architectures, hICN and CONET, in subsection 4.2.

4.1 Features to be Analysed

In order to investigate S&P features, general ICN characteristics were studied, presented in the following subsection. After the ICN characteristics, S&P features are provided, that were examined in the chosen architectures.

4.1.1 ICN Features

This section states the basic features discussed in this paper, namely *Naming, Forwarding, Caching, and Security* followed by a brief description of each. The inspiration for the list drawn from [22].

Naming The naming schemes can be divided into three groups: hierarchical, self-certifying and attribute-value pair [22].

- Hierarchical: These are non-persistent but usually human friendly names which are formed by multiple hierarchical components.
- Self-certifying: These are persistent and unique names, composed of two parts *<P:L>*. P is the cryptography hash of the owner's public key and L is a content label assigned by the owner. Meta-data contains the full public key and digital digest signed by the owner.
- Attribute-value pair: The names do not have to be unique and do not ensure security of the content names. Each attribute contains the name, a type and a set of possible values.

Routing Routing can be divided into two categories namely name resolution and name-based routing. [11]

- Name resolution: In this approach the name is resolved to a single/set of IP address/es. Then a topology based shortest path routing is used, to request the desired IP addresses.
- Name-based routing: Requests are directly routed based on the content name. State information is stored along the way, that is used to deliver content using the reverse path.

Caching On receiving a request a router may have cache data that could be transferred directly, otherwise, it requests the content from its peer/s. ICN allows for pervasive caching, which is uniform for all protocols, and content delivery from all users regardless of the type of content or the status of the user. [23].

Content-Centric Security ICN architectures are focused on content-centric security that ensures the security of the content itself, unlike the present internet architecture, which is based on host-centric security. A host-centric security model requires trust in the location of the content and the medium of travel, which is difficult to enforce in ICN. Due to caching the user can use any available copy of the content regardless of its previous whereabouts [24].

4.1.2 Security and Privacy Features

This section present the privacy and security features which were investigated in the selected architectures. These traits are divided into two categories *Security* and *Privacy.*

Privacy

- ***Anonymity*** ensures that the identity of any user in the network is not revealed [25]. With the current IP protocols, users make requests with their IP address and that of the destination, which reveals their identity to the sniffers on the network. Whereas ICN allows any user to send a request, or requested data without being identified by others on the network.

- ***Confidentiality*** is to make sure that only qualified entities can access secured information, and that data remains a secret during transit [22]. Current IP protocol relies on encrypted connections to ensure confidentiality. ICN allows users to request data based on its name, and security lies in the packets containing it. To ensure confidentiality, it would mean to add another layer of privacy by the producer to grant access to only a certain group of consumers [4].

- ***Unlinkability*** Unlinkability assures that a single or a group of requests can not be linked to any user of the network or each other, which would put the identity of a user at risk[25]. Moreover, the requests or the requested data packets are not linked to each other to reveal anything about the users [25]. As requests are made with names in ICN, warranting unlinkability would mean that the names do not resolve to reveal a userâs identity.

Security

- ***Availability*** ensures that the objects published in the network have to be available and accessible. [22]. In terms of ICN, it would mean that all users should be able to request any content on the network with the correct name or label.

- ***Access Control*** is limiting and controlling the access of a user on content based on their rights [4]. In IP Protocol, it is ensured by the connection between the data provider and requester is established after authentication. Due to the content-centric nature of ICN, where data can be cached on any router or device, access control is not inherently present and can be ensured by encrypting data.

- ***Non-repudiation*** is preventing the ability to deny ownership over content in the network [26]. Provenance gives confidence to the consumer that the producer of the content is trustful. The data may or may not be supplied from the producer in ICN due to its content-centric nature. Non-repudiation ensures that the requester gets the content generated from a reliable source.

- ***Integrity*** means the ability to identify any accidental or intentional changes to information objects and the corresponding metadata [22]. The data in an ICN network gets cached or travels through various intermediate devices. Therefore, it is essential for a user to be able to verify that it is not tampered with.

- ***Authentication*** deals with verifying the provider and assuring the requester of the content. That can be seen as a parameter to verify the origin of requested content [4]. This parameter provides users to verify that a certain piece of data is provided from the source where it claims to be from. This trait can be seen as a mix of integrity and non-repudiation.

4.2 Investigation of Hybrid Architectures

This section presents the features implemented based on the list given in section 4.1. Consequent subsections, 4.2.1 and 4.2.2, are about hICN and CONET respectively, each subsection first reviews the general ICN traits and then the Security and Privacy features with their implementation.

4.2.1 hICN

Overview of ICN features

Naming hICN follows hierarchical naming, which allows for better scale routing, as it uses name aggregation and defines lower indexes [27]. Routing by name aggregation enables hICN architectures to reduce redundant requests as multiple requests for the same data can be reduced to a single request. In hICN, each piece of data-name consists of two parts, a name prefix and a name suffix [16]. The name prefix is used for forwarding, whereas the suffix contains transport information. Hence, the IPv6 header field is made from the prefix, encoded as 128 bits word. Meanwhile, the suffix is added to the transport headers field, such as TCP.

Routing Name-based routing is employed by hICN. Requests packets received at a router are forwarded or responded to with data packets depending on if the router has a copy of the requested data [28]. If the requested data is not available, the router performs a name-based Longest Prefix Match lookup in FIB to forward the packet to the next router. If the requested data is present, then the reply is forwarded to the identifier present in the source address field of the request packet. For further details on routing refer to [28]

Caching A router's local memory is used for temporarily storing interest or data packets. When a router receives a request, it is stored in the caching data structure to revert the acknowledgment or the reply when found [16]. Then a lookup is performed in the CS to check if the requested data is already present in cache memory. For cache lookup, the full name of the requested data is used, unlike the lookup for routing where only the prefix is used. Cache memory is indexed with full names, concatenation of prefix, and suffix.

Content-Centric Security hICN applies the Content-Centric Security model to secure the content being transferred rather than focusing on securing the medium [16, 10]. hICN inherits the IP Authentication Header (IP AH) and Transport Manifest from the existing protocols [16]. IP AH is added after the transport layer, that is after the TCP header.

IP AH is not an extension to the IPv6, hence, avoiding packets from being filtered by the network devices. For the packets to be verifiable, the signature of IP AH is computed over the immutable extension fields of the packet. Transport Manifest carries the metadata on the group of data packets to convey to the consumer. It also carries cryptographic hashes of data packets computed over immutable fields, same as in IP AH. The manifests are also signed by the producer, providing another layer of security, verifiable by the consumer.

Overview of Security and Privacy Features

Privacy Features

- *Anonymity*: hICN provides anonymity to its users in the network. The packets transferred over the network do not carry information about the receiver of that packet. hICN inherits IPv6 protocol, traditional IP packets carry the IP address of the source or the destination. However, with hICN, these are replaced by the prefix of the content name [17]. The identities of the devices on the route are used only in-between hops, therefore it is difficult to identify the requester or the sender.

- *Confidentiality*: Due to the absence of a central host to provide content and the presence of caching, confidentiality is not inherently present for hICN packets. Nevertheless, optionally can be applied by the users with encryption. The content transferred can be encrypted by the producer for an additional level of security which could be decrypted only by the appropriate keys [29, 30].

- *Unlinkability*: Partial unlikability, as all the requests carry information of the data to be requested or received and have no link to the users providing or requesting them. It is partial as the requests for the same content can be linked together, as the prefix is mentioned in the packet. During routing the packets are stored in FIB, CS, and PIT, with their content names rather than IP addresses. Hence, ensuring that none of the packets can be linked back to any user.

Security Features

- *Availability*: Due to the content-centric nature, all the data packets are available to the users if they have the correct data name to request them. Data packets are available to and verifiable by the consumers [16]. In the case of encrypted payload, the consumers with valid decrypting keys would be able to access the data.

- *Access Control*: It is not inherently present in hICN as explained in section 4.1.2. Hence, hICN does not have any additional parameters to support access control. However, additional encryption can be applied to the data, and decrypting keys can be distributed to the eligible users.

- *Non-repudiation*: Authentication Header carries the signature of the producer, which provides the authenticity of data origin [31]. The transport manifest is signed with the producerâs private key [17]. The signature is verifiable by the consumer. Hence, giving confidence to the producer of the content.

- *Integrity*: AH has an Integrity Check Value field that is computed over the packet, which includes the payload. It also provides an algorithm to calculate this value at the consumer's endpoint over the received packet to ensure data integrity [31, 17]. Therefore integrity is ensured in hICN packets.

- *Authentication*: Authentication is the verification of the provider of the content and assurance of the content provided to the requester. As these are covered in integrity and non-repudiation, therefore authentication is also covered by hICN architecture.

4.2.2 CONET

Overview of ICN Features

Naming Self-certifying names are used to form content names in CONET. Usually, there's a network identifier in form of a tuple, *<namespace ID, name>* [18]. The namespace ID gives the specifications on the format of the name. Each namespace has its own formatting rules to form unique names. Each name is composed of two hash values, *name = <hash(Principal), hash(Label)>* where Principal and Label are flat-names. A principal is the owner of the named-data and has a unique hash in a namespace known as a principal identifier. Meanwhile, a label is an identifier for the data chosen by the Principal and is unique in that namespace.

Routing Name-based routing is employed in CONET. The routing table, FIB is the same as that in traditional IP routers, except that it is populated with name prefixes i.e. *<network-identifier, mask>* rather than net-prefixes [19, 18]. FIB uses a function to resolve namespace ID to next-hop address, which is an address of a node in that CSS or address to BN of a different CSS.

Caching Caching takes place only in ENs, INs, and BNs. On receiving a request, the node checks if the requested data is available in its cache memory, if it is, then the node responds with that cache content [18]. For caching memory, a separate CPU is reserved at the router that performs caching algorithm.

Content-Centric Security CONET inherits the Content-Centric Security model, where securing the content is prioritized over securing the network. CONET follows self-certifying names, where names are a tuple, *< hash(principle), hash(label)>* [18, 19]. The content owner is a principal and selects a label for its content. There's a mapping from label to content, that can be used by the consumer for verification [29].

Overview of Security and Privacy Features

Privacy features

- *Anonymity*: The packets do not carry any information about who requested the data or the final destination [18, 32]. Unlike the IP packets, the IP addresses are replaced by the name of the data being requested or carried. The intermediate BN receives the address of the BN of the earlier CSS to enable backward routing when requested data is found. Consequently, ensuring anonymity of the users.

- *Confidentiality*: As seen in hICN, CONET likewise does not inherently support confidentiality for the same reason mentioned in section 4.2.1. However, the data can be encrypted by the producer, then users only with the appropriate key would be able to access it [18, 29].

- *Unlinkability*: There are various nodes or CSSs involved in the routing process of CONET. To satisfy a data request, a CIU may pass several CSSs. The packet is passed from one CSS to another by BNs, and the immediate BNs receive the address of the previous BN for sending requested data or acknowledgment backward on the same route [32, 20]. Nodes on the route do not pass the IP address of the final destination while routing, so a CIU can not be linked back to a requester or provider of the content. Nevertheless, the CIU for the same data may be linked to each other due to the same labels. Therefore, CONET supports partial unlinkability.

Security features

- *Availability*: Any user can generate a request for content on the network with the correct name. Trust relies upon the content rather than the network. Therefore, it is openly available [18]. Any user can access the content except when data is encrypted.
- *Access Control*: Like hICN, CONET also does not provide access control due to the content-centric nature of the architecture, as explained in section 4.1.2. Nevertheless, like in hICN, the data can be encrypted to allow some sort of access control [29].
- *Non-repudiation*: As mentioned in naming, CONET utilizes tuple <*Principal, Label*> in the naming schema. The Principal is signed by the creator of the content, providing non-repudiation [29, 19].
- *Integrity*: Self-verifying names give confidence about the integrity of the content. As matching between content offered and its name shows that the content is not tampered with [29]. The mapping can be publicly made available in the network and fetched with named-data. Additional metadata for the matching is also present as *security-data* in the CIUs.
- *Authentication*: As mentioned previously in section 4.2.1, authentication is covered by integrity and non-repudiation. Naming used for CIU packets is self-certifiable, offering integrity, and the signed *Principal* by the creator assuring provenance [29, 19]. Therefore, CONET supports authentication.

5 Discussion

Table 1: Security & Privacy features in the hybrid architectures

Security Features	hICN	CONET
Availability	Supported	Supported
Access Control	Not supported	Not supported
Non-repudiation	Supported	Supported
Integrity	Supported	Supported
Authentication	Supported	Supported

Privacy Features	hICN	CONET
Anonymity	Supported	Supported
Confidentiality	Not supported	Not supported
Unlinkability	Partially supported	Partially supported

This paper focused on investigating the security and privacy features in hybrid ICN architectures. The conclusions of this report are drawn from the examination of two hybrid architectures with similar functionality but different implementations. This section is centered on exhibiting a comparison between the two architectures after the results in section 4.

Comparison on deployment: ICN features are intrinsically present in both the architectures, also supporting the current IP protocol. Still, there lies a difference in their deployment as hICN routers can be seen as standalone routers, which can be deployed in the current network [14, 16]. Meanwhile, CONET requires a standardization of the routers or devices in the network. As the native IP routers might end up being intermediate nodes between CSSs, they have to be configured such that packets with unknown IP options are not dropped [16].

Comparison on privacy features: After the results presented in the previous section, it is safe to say that anonymity is inherently present in most of the ICN architectures if they work on name-based routing and caching is employed. Name-based forwarding ensures independence from IP addresses. As the IP address fields are manipulated to store the names of the content requested or delivered, also due to caching, it is difficult to identify the final destination of the packet. Packets or CIUs carry the IP addresses of the nodes immediately next to them, that is one before or one next in the hop. Assuring that data requests are unlinkable to any user in the network. One may argue that hybrid architectures would provide partial unlinkability, as packets or CIUs for the same data may or may not be linked together depending upon the architecture's implementation. For the two architectures covered in this paper, it is hard to form any conclusion if they support unlinkability between the packets or CIUs. IP protocol assures confidentiality if need be by enabling encryption in the channel between consumer and server. However, it is difficult to achieve with the content-centric nature of ICN. For the discussed two architectures, no inherent features are present to ensure confidentiality. Nonetheless, data could be encrypted by the producer to provide some sort of confidentiality.

Comparisons on security features: After discussing the privacy feature, we move the focus to the security features. Availability can be said to be inherently present in all hybrid architectures, given name-based routing is employed. One may argue that confidentiality goes against availability, but that is not the case. As any user on the network can fetch any data packet, but may not be able to access the payload if data is encrypted. As confidentiality is not inherently present, access control is also missing and may be implemented by encrypting data on different levels. Accordingly, users would be able to encrypt certain parts of data depending upon their access rights. So far, both the architectures have exercised the privacy features and availability in a very similar manner. The last three security features: non-repudiation, integrity, and authentication, are all ensured with the data-centric security model involved in both hybrid architectures discussed in this paper. It is interesting to note the difference in the implementation of data-centric security. CONET depends on its data naming strategy, whereas hICN inherits the current IP AH and Transport Manifest. Of course, IP AH and Transport Manifest fields are tweaked to ensure the security of the packet itself, independent from the channel's security. Meanwhile, CIUs provide consumers with algorithms to compute on the name to ensure integrity and provenance.

6 Reliability, Validity and Ethicality

This section discussed the reproducibility of the results and presents a discussion about the ethical controversies attached to the speedy rollout of ICN with hybrid architectures.

The methodology presented in section 3 gives an overview of how the material for the research was collected, ensuring the reproducibility of the results. The given keywords were used to find reliable sources from ScienceDirect, IETF, IEEE, and ACM. The validity of other material used in this research was checked by comparing the architectural description presented in the internet-draft found on IETF, due to its authenticity for IoT. The most latest published resources were used as IoT keeps evolving. There is not much development on the CONET architecture after the European CONVERGENCE project [9], most of the material date back to 2014. On the other hand, hICN is openly available to use and test, as CISCO is pushing for its development to ease the roll-out of 5G [10].

The deployment of hybrid ICN architectures would make ICN benefits openly available to the users but like all other technologies, pros come at a cost. These costs should not be brushed off for the sake of the development of the technology. One of the major benefits is anonymity, which would probably remove one's reliability on Virtual Private Networks (VPN)s [33]. The independence from IP addresses definitely encourages freedom of speech [34] though also disrupts the current law enforcement's dependency on geo-location to track criminal behavior such as pirating copyrighted content [35]. Name-based routing and in-router caching for sure would democratize content distribution [33]. However, it would difficult to hold someone responsible for taking down illegitimate content from cache storage of millions of devices or routers [36]. Consequently, deployment of the hybrid architectures should take place taking the cons into account and mitigating as many as possible.

7 Conclusions and Future Work

The aim of this paper was to analyze two hybrid ICN architectures, hICN and CONET, to assess their S&P features. In order to properly assess these architectures, the implementation and working of ICN characteristics were examined. hICN architecture can be deployed easily, whereas CONET requires standardization in routers so that CIUs are not dropped en route. It is interesting to note that CONET uses self-certifying names that also allow it to implement content-centric security. Whereas hICN has hierarchical naming and inherits AH and transport manifest from the current internet infrastructure to ensure content-centric security. Examination of ICN characteristics allows understanding the implementation of S&P features in the two architectures. Both the architectures support the same features but from different implementations, also both miss out on Access Control and Confidentiality. The content-centric nature of ICN makes it difficult to implement traditional Confidentiality and Access Control where the restrictions are imposed by a central host. Nonetheless, these two traits can be employed by encrypting data and distributing encryption keys to eligible consumers. The results drawn in this paper are from a literature review of the two architectures, providing a thorough study of the two architectures and a general overview of hybrid architectures. However, this paper does not represent the traits of all the architectures following the hybrid approach. To gain a general overview of hybrid architectures, more architectures should be studied. Furthermore, the results drawn from this paper could be employed to find the gaps in S&P features covered in the mentioned two architectures to further improve upon.

References

[1] Vint Cerf. *A Brief History of the Internet & Related Networks.* en-US. URL: https://www.internetsociety.org/internet/history-internet/brief-history-internet-related-networks/.

[2] Athanasios V. Vasilakos et al. "Information centric network: Research challenges and opportunities". en. In: *Journal of Network and Computer Applications* 52 (June 2015), pp. 1–10. ISSN: 1084-8045. DOI: 10.1016/j.jnca.2015.02.001. URL: https://www.sciencedirect.com/science/article/pii/S1084804515000272.

[3] Laura Heath et al. "CLIP: Content labeling in IPv6, a layer 3 protocol for information centric networking". In: *2013 IEEE International Conference on Communications (ICC).* ISSN: 1938-1883. June 2013, pp. 3732–3737. DOI: 10.1109/ICC.2013.6655135.

[4] Jonathan Loo and Mahdi Aiash. "Challenges and solutions for secure information centric networks: A case study of the NetInf architecture". en. In: *Journal of Network and Computer Applications* 50 (Apr. 2015), pp. 64–72. ISSN: 1084-8045. DOI: 10.1016/j.jnca.2014.06.003. URL: https://www.sciencedirect.com/science/article/pii/S1084804514001337.

[5] Mauro Conti et al. "The Road Ahead for Networking: A Survey on ICN-IP Coexistence Solutions". en. In: *IEEE Communications Surveys & Tutorials* 22.3 (2020), pp. 2104–2129. ISSN: 1553-877X, 2373-745X. DOI: 10.1109/COMST.2020.2994526. URL: https://ieeexplore.ieee.org/document/9094202/.

[6] A. Rahman et al. *Deployment Considerations for Information-Centric Networking (ICN).* en. Tech. rep. RFC8763. RFC Editor, Apr. 2020, RFC8763. DOI: 10.17487/RFC8763. URL: https://www.rfc-editor.org/info/rfc8763.

[7] Hao Wu et al. "On Incremental Deployment of Named Data Networking in Local Area Networks". In: *2017 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS).* May 2017, pp. 82–94. DOI: 10.1109/ANCS.2017.18.

[8] R. Tourani et al. "Security, Privacy, and Access Control in Information-Centric Networking: A Survey". In: *IEEE Communications Surveys Tutorials* 20.1 (2018). Conference Name: IEEE Communications Surveys Tutorials, pp. 566–600. ISSN: 1553-877X. DOI: 10.1109/COMST.2017.2749508.

[9] *The Convergence Project.* URL: http://www.ict-convergence.eu/.

[10] Luca Muscariello. *Cisco Advances Open-Source Hybrid Information-Centric Networking for 5G.* en-US. Feb. 2019. URL: https://blogs.cisco.com/innovation/cisco-advances-open-source-hybrid-information-centric-networking-for-5g.

[11] Bengt Ahlgren et al. "A survey of information-centric networking". en. In: *IEEE Communications Magazine* 50.7 (July 2012), pp. 26–36. ISSN: 0163-6804. DOI: 10.1109/MCOM.2012.6231276. URL: http://ieeexplore.ieee.org/document/6231276/.

[12] Bastiaan Wissingh et al. “Information-Centric Networking (ICN): CCNx and NDN Terminology”. en. In: *undefined* (2020). URL: /paper/Information-Centric-Networking-(ICN)%3A-CCNx-and-NDN-Wissingh-Afanasyev/c00a2335c015ac1881d03bee43a8b41d54f9140a.

[13] Ikram Ud Din et al. “Caching in Information-Centric Networking: Strategies, Challenges, and Future Research Directions”. en. In: *IEEE Communications Surveys & Tutorials* 20.2 (2018), pp. 1443–1474. ISSN: 1553-877X. DOI: 10.1109/COMST.2017.2787609. URL: https://ieeexplore.ieee.org/document/8240926/.

[14] CISCO. *Hybrid Information-Centric Networking â Hybrid ICN 20.01 documentation.* Documentation. 2017. URL: https://fd.io/docs/hicn/latest/.

[15] Davythe Dicochea. “Mobile Video Delivery with Hybrid ICN”. en. In: *CISCO* (2017).

[16] G Carofiglio et al. “Enabling ICN in the Internet Protocol: Analysis and Evaluation of the Hybrid-ICN Architecture”. en. In: (2019), p. 20.

[17] Luca Muscariello et al. *Hybrid Information-Centric Networking.* Internet-Draft draft-muscariello-intarea-hicn-04. Work in Progress. Internet Engineering Task Force, May 2020. 22 pp. URL: https://datatracker.ietf.org/doc/html/draft-muscariello-intarea-hicn-04.

[18] Andrea Detti et al. “CONET: a content centric inter-networking architecture”. In: *Proceedings of the ACM SIGCOMM workshop on Information-centric networking.* ICN ’11. New York, NY, USA: Association for Computing Machinery, Aug. 2011, pp. 50–55. ISBN: 978-1-4503-0801-4. DOI: 10.1145/2018584.2018598. URL: https://doi.org/10.1145/2018584.2018598.

[19] Andrea Detti, Stefano Salsano, and Nicola Blefari-Melazzi. *IP protocol suite extensions to support CONET Information Centric Networking.* Internet-Draft draft-detti-conet-ip-option-05. Work in Progress. Internet Engineering Task Force, June 2013. 21 pp. URL: https://datatracker.ietf.org/doc/html/draft-detti-conet-ip-option-05.

[20] N. Blefari Melazzi et al. “An OpenFlow-based testbed for information centric networking”. In: *2012 Future Network Mobile Summit (FutureNetw).* July 2012, pp. 1–9.

[21] Boubakr Nour et al. “Coexistence of ICN and IP Networks: An NFV as a Service Approach”. In: *2019 IEEE Global Communications Conference (GLOBECOM).* ISSN: 2576-6813. Dec. 2019, pp. 1–6. DOI: 10.1109/GLOBECOM38437.2019.9013881.

[22] Eslam G. AbdAllah, Hossam S. Hassanein, and Mohammad Zulkernine. “A Survey of Security Attacks in Information-Centric Networking”. en. In: *IEEE Communications Surveys & Tutorials* 17.3 (2015), pp. 1441–1454. ISSN: 1553-877X. DOI: 10.1109/COMST.2015.2392629. URL: http://ieeexplore.ieee.org/document/7009958/.

[23] Ali Ghodsi et al. “Information-centric networking: seeing the forest for the trees”. en. In: *Proceedings of the 10th ACM Workshop on Hot Topics in Networks - HotNets ’11.* Cambridge, Massachusetts: ACM Press, 2011, pp. 1–6. ISBN: 978-1-4503-1059-8. DOI: 10.1145/2070562.2070563. URL: http://dl.acm.org/citation.cfm?doid=2070562.2070563.

[24] B. F. Wissingh et al. *Information-Centric Networking (ICN): Terminology.* en. Mar. 2017. URL: https://tools.ietf.org/id/draft-wissingh-icnrg-terminology-01.xml.

[25] Tianbo Lu, Zeyu Du, and Z. Jane Wang. "A Survey on Measuring Anonymity in Anonymous Communication Systems". In: *IEEE Access* 7 (2019). Conference Name: IEEE Access, pp. 70584–70609. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2919322.

[26] Zachary Zeltsan. *ITU-T Recommendation X.805 and its application to NGN*. en. Apr. 2005.

[27] *A transport layer and socket API for (h)ICN*. DOI: 10.1145/3267955.3267972. URL: https://dl-acm-org.tudelft.idm.oclc.org/doi/epdf/10.1145/3267955.3267972.

[28] Jordan Auge et al. *Anchorless mobility through hICN*. Internet-Draft draft-auge-dmm-hicn-mobility-04. Work in Progress. Internet Engineering Task Force, July 2020. 28 pp. URL: https://datatracker.ietf.org/doc/html/draft-auge-dmm-hicn-mobility-04.

[29] Van Jacobson and Diana Smetters. "Securing Network Content". en. In: *Palto Alto Research Center* (Jan. 2009).

[30] Cesar Ghali, Gene Tsudik, and Christopher A. Wood. "(The Futility of) Data Privacy in Content-Centric Networking". In: *Association for Computing Machinery*. WPES '16 (Oct. 2016). DOI: 10.1145/2994620.2994639. URL: https://dl.acm.org/doi/epdf/10.1145/2994620.2994639 (visited on 06/03/2021).

[31] Stephen Kent. *IP Authentication Header*. RFC 4302. Dec. 2005. DOI: 10.17487/RFC4302. URL: https://rfc-editor.org/rfc/rfc4302.txt.

[32] J. Doe. *IPv4 and IPv6 Options to support Information Centric Networking*. en. Dec. 2010. URL: https://tools.ietf.org/id/draft-detti-conet-ip-option-02.html#CONET11.

[33] Katie Shilton et al. "Anticipating policy and social implications of named data networking". In: *Communications of the ACM* 59.12 (Dec. 2016), pp. 92–101. ISSN: 0001-0782. DOI: 10.1145/2915915. URL: http://doi.org/10.1145/2915915.

[34] David J. Phillips. "From Privacy to Visibility: CONTEXT, IDENTITY, AND POWER IN UBIQUITOUS COMPUTING ENVIRONMENTS". In: *Social Text* 23.2 (83) (June 2005), pp. 95–108. ISSN: 0164-2472. DOI: 10.1215/01642472-23-2_83-95. URL: https://doi.org/10.1215/01642472-23-2_83-95.

[35] Louise Cooke. "Controlling the net: European approaches to content and access regulation". en. In: *Journal of Information Science* 33.3 (June 2007). Publisher: SAGE Publications Ltd, pp. 360–376. ISSN: 0165-5515. DOI: 10.1177/0165551506072163. URL: https://doi.org/10.1177/0165551506072163 (visited on 06/19/2021).

[36] Patrick Kwadwo Agyapong and Marvin Sirbu. "Economic incentives in information-centric networking: implications for protocol design and public policy". In: *IEEE Communications Magazine* 50.12 (Dec. 2012). Conference Name: IEEE Communications Magazine, pp. 18–26. ISSN: 1558-1896. DOI: 10.1109/MCOM.2012.6384447.