Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777661

INFORMATION CENTRIC NETWORKS AND ITS SECURITY CHALLENGES

Aravinda Thejas Chandra
Associate Professor, Dept of ISE, SJCIT, Chickballapur, India
thejaschandra@sjcit.ac.in

Dr Rajashekara Murthy
Associate Professor, Dept of ISE, RVCE , Bengaluru, India
rajashekaramurthys@rvce.edu.in

Abstract

An new networking discipline called "information centric networking" (ICN) has the power to completely alter how the Internet functions. ICNs allow users to immediately access content from anywhere on the network, regardless of its physical location, by identifying each item of information by its name instead by the destination host to which it will be routed over the network. This makes ICN networks more scalable, secure, and efficient. However, since ICN infrastructure is still a relatively new technology, it faces several security challenges. These include the threat of privacy breach, spoofing, distributed denial-of-service attacks, and the inadequate authentication protocol. To ensure that ICN networks' full potential be realised, these security issues will need to be resolved. The delivery of content within a network, as opposed to a specific device, is the main goal of information centric networking (ICN), communications architecture. By letting the network to use content as the fundamental unit of transport rather than the conventional end-points, this developing network architecture seeks to enhance the existing Internet routing model. The purpose of ICN is to offer an improved and more secure framework for the delivery of content over the Internet. An Information Centric Network (ICN) is an architecture that utilizes an indexed structure for the dynamic distribution of digital content. This structure allows nodes within the network to send and query for content based on user-defined keywords and topics, rather than relying solely on the IP addresses of network endpoints. This approach provides a more efficient and reliable method of content delivery, as it becomes easier to locate, route, and deliver digital content irrespective of its source or destination. Security is an essential component for any network and is especially important for Information Centric Networks because the increased complexity of the network structure introduces new attack surfaces and an increased reliance on caching. Attacks like denial-of-service attacks, cache poisoning, packet replay, and other forms of malicious behaviour are among the security difficulties faced by ICNs. **More security measures are required to** protect against these types of attacks, including mechanisms such as encryption, authentication, and authorization. Additionally, secure content distribution needs to be established in order to prevent malicious entities from accessing or altering content data. As networks complexity continues to increase and more data is digitized, security needs to remain a top priority in order to protect the integrity of networks, services, and content.

Keywords:
Information-Centric Networking, Security, Challenges, Data, Internet, Performance

I. Introduction

The rapid development of communication technologies and the widespread adoption of mobile devices have resulted in a significant increase in internet usage.. Due to this rise in content consumption, the idea of the information-centric network (ICN)1-4 as a type of internetworking was born. Social media sites' popularity and growing use for information retrieval also contribute to a growth in their volume.

This new networking approach puts more emphasis on content than hosts. ICN does not necessitate a client visiting the content producer in order to obtain the desired data, in contrast to host-centric IP networks. The requested content can be delivered to the client by any networked device [1]. To provide content-oriented access, the ICN architecture offers various features, including name-based self-secured content sharing, caching, and distinctive content naming. Caching is a noteworthy and important element of ICN that permits named content serving from intermediate storage.

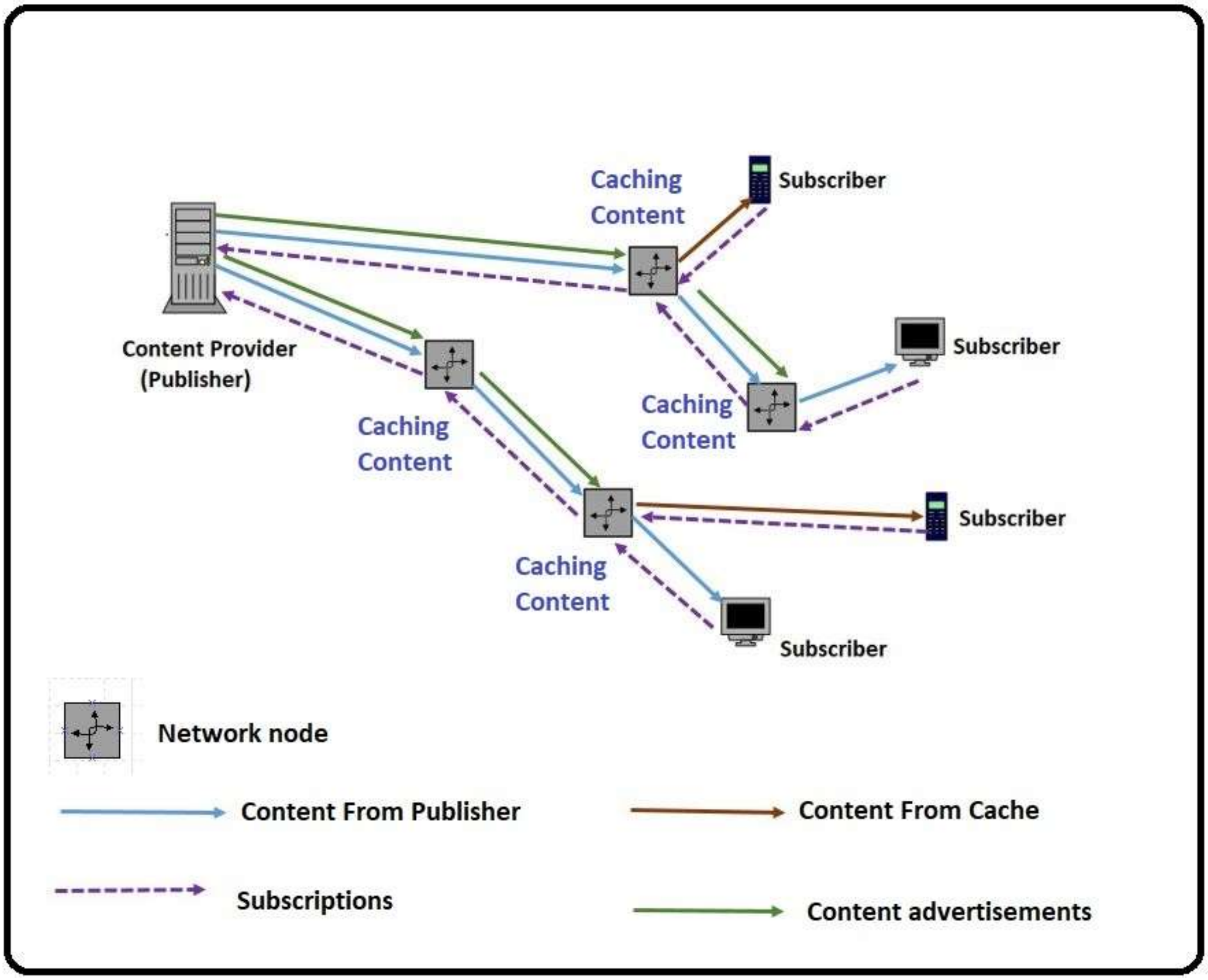

FIG1: Basic Operation of ICN

Since hosts can be contacted widely, are widely known, and can be addressed specifically, hosts are the primary focus of the conventional Internet [2]. ICN advises that every piece of content intended for general access be individually labelled and completely searchable by name. Intermediate router caching additionally quickens the delivery of material to users [3]. This reduces end-to-end delay and network utilization, but it also presents several design and deployment issues. It is only possible to store some single pieces of data because of the limited storage in intermediate routers. Therefore, an effective caching mechanism is crucial to improving ICN performance.

The research and development community's efforts over the past 10 years have made significant advancements in the implementation of high-quality, high-performance, and functionally robust ICN networks [4], [5]. Additionally, the security of ICN is very well examined with a focus on particular attacks [6], [7] and countermeasures [8]–[11]. Many protocols, including SNMP and ICMP, keep track of the network to make finding and configuring network nodes and aggregating monitoring data simple [12]-[16].

Simply monitoring a network is insufficient to evaluate its level of security. Security assurance is a common practice used to enhance the security status of a targeted system and provide credible assurance that it will perform as intended despite errors and attacks. Certification is a preferred approach to security assurance in which system data is gathered to demonstrate a particular attribute. The data collected is then used to issue a certificate confirming specific properties of the system. Certification schemes is used not only in traditional software but also in web and cloud services [16], and as intricate service compositions. Monitoring, testing, or formal proofs are employed to gather evidence in these scenarios [17]. Modern certification methods are dynamic, continuous, and lightweight, possessing unique attributes that make them suitable for validating even complex network protocols [18].

ICN certification and security assurance are, as far as we know, still in their infancy. Information-centric networks' lack of openness and reliability becomes a major impediment to their widespread adoption and can allow for persistent threats with the potential to significantly change network behaviour. Additionally, the operation of the entire network can be hampered by system flaws and vulnerabilities to poisoning attacks, [11].

II. History of ICN

The history of Information-Centric Networking (ICN) is closely intertwined with the efforts of various organizations, research groups, and standardization bodies[19]. Here, we will explore the contributions of TRIAD, IRTF, and ICNRG in shaping the development and advancement of ICN.

TRIAD (Towards Robust Information Access Distribution): TRIAD was a project funded by the European Commission . It aimed to investigate the concepts of ICN and develop a robust architecture for information-centric networking. The project commenced in 2010 and involved collaboration between leading research institutions and industry partners across Europe.

TRIAD focused on challenges like scalable content delivery, in-network caching, and dynamic content dissemination. The project developed prototypes and conducted experiments to evaluate the feasibility and performance of ICN principles in real-world scenarios.

The outcomes of TRIAD significantly contributed to the advancement of ICN, providing valuable insights, architectural designs, and practical implementations.

IRTF (Internet Research Task Force is an open global community composed of researchers, academics, and industry experts. Established in 1989, the IRTF operates under the Internet Architecture Board (IAB) and focuses on long-term research topics related to the evolution and development of the Internet.

Within the IRTF, the ICN Research Group (ICNRG) was formed in 2013 to specifically address ICN-related research challenges. The ICNRG serves as a platform for researchers and practitioners to collaborate, exchange ideas, and contribute to the advancement of ICN.

The ICNRG organizes regular meetings, workshops, and discussions to explore ICN concepts, identify research gaps, and propose solutions. The group has released a multitude of research papers, RFCs (Request for Comments), and informational documents that have shaped the understanding and development of ICN.

ICNRG actively collaborates with other standardization bodies, research communities, and industry stakeholders to promote ICN as a viable networking paradigm for the future Internet.

Contributions to ICN Standardization: Standardization plays an important role in adoption and interoperability of networking technologies. ICN has garnered attention within standardization bodies, and efforts have been made to define specifications and protocols for ICN.

The ICNRG, operating under the IRTF, has actively contributed to ICN standardization. Through its working groups and discussions, the ICNRG has provided valuable input and recommendations for the development of ICN-related standards.

In addition to the ICNRG, other standardization bodies, such as the Internet Engineering Task Force (IETF), have also recognized the importance of ICN. The IETF has initiated efforts to explore ICN concepts, challenges, and potential protocols through working groups and research activities.

These standardization efforts aim to define common protocols, mechanisms, and interoperability guidelines for ICN, paving the way for its widespread adoption and deployment.

In summary, TRIAD, IRTF (specifically the ICNRG), and ICN standardization bodies have played significant roles in the history of ICN. Their research, collaboration, and standardization efforts have advanced the understanding, development, and deployment of ICN as a promising networking paradigm.

Table 1: Comparison of ICN Architectures

Sl No	Architecture	Active Years	Original	Main Points	Drawbacks
	DONA	2007 -		Introduces Information	-Limited deployment

1		present	http://www.sigcomm.org/node/2633 University California Berkeley	Objects (IOs) as the fundamental units of ICN. - Focuses on a scalable and robust naming architecture using a distributed hash table (DHT) to store and retrieve IOs. - Emphasizes security and privacy aspects with access control and encryption mechanisms .	and adoption - Lack of a centralized naming authority could lead to naming conflicts.
2	NDN	2010 - present	https://named-data.net/project/ndn/	Emphasizes the concept of named data, where content is accessed by its name rather than location. - Supports in-network caching and hop-by-hop Interest/Data exchange. - Implements a	-Requires changes to existing applications to adopt the NDN communication model. - Scalability challenges with large-scale content distribution.

				hierarchical naming scheme. - Provides security through signatures and access contro	
3	CCN	2009 - 2014	RFC 8569	Proposes a content-centric network architecture where content is the primary focus. - Utilizes content names for routing and caching. - Supports in-network caching and content retrieval based on Interest/Data exchange. - Implements signature-based security mechanisms	-Limited deployment and development due to the end of its initial research phase. - Lack of widespread community support.
4	MobilityFirst	2011 - 2017	https://mobilityfirst.winlab.rutgers.edu/	Addresses mobility challenges in ICN by incorporating the mobility of	Limited deployment and adoption. - Requires changes to existing

				network entities. - Enables seamless mobility and location-independent communication. - Introduces identifiers for naming mobility entities. - Implements a distributed architecture with distributed caching.	network infrastructure and devices to support mobility-first communication.
5	NetInf	2007 - 2013	https://www.sail-project.eu/about-sail/netinf/index.html	Focuses on information-centric networking by decoupling information from location. - Uses globally unique identifiers (GUIDs) to retrieve and cache information. - Supports distributed caching and content-based routing. -	Limited development and deployment. - Lack of widespread community support. - Scalability challenges with large-scale content distribution.

				Incorporates security and privacy mechanisms.	
6	CONVERGENCE	2011 - 2014	http://www.ict-convergence.eu/ European Funded FP7 Project	Aims to integrate ICN with existing IP networks to leverage the advantages of both paradigms. - Focuses on seamless integration, security, and scalability. - Proposes protocols for interworking between ICN and IP networks. - Supports in-network caching and content retrieval.	Limited deployment and development. - Challenges in interworking between ICN and IP networks. - Scalability concerns with the integration of two network paradigms.
7	PURSUIT	2008 - 2011	http://www.fp7-pursuit.eu/ (Europe)	Proposes a clean-slate design for ICN to address issues in current network architectures. - Focuses on security, trust, and privacy	Limited development and deployment. - Lack of widespread community support. - Challenges in practical implementation and adoption. -

				aspects. - Incorporates self-organizing principles. - Supports in-network caching and routing. - Emphasizes security and privacy through cryptographic mechanisms.	Scalability concerns in large-scale networks. - Lack of real-world deployment and evaluation. - Complex cryptographic requirements.

III. ICN Architectures

The open-source implementation of ICN, which outlines a thorough naming scheme, content retrieval storage, and dissemination algorithms, served as a model for the NDN project and other initiatives that advocate for a comprehensive networking protocol. As a result, we outline the architecture and process of various ICN approaches in this subsection.

- NDN
- CCN
- PURSUIT
- Mobility First
- CONVERGENCE
- NetInf
- DONA

Information Centric Networking (ICN) is a network architecture that concentrate on content as the primary entity rather than hosts or locations. In ICN, content is accessed by its name, and the network infrastructure handles the task of retrieving the content from the most suitable source. Many ICN approaches have been developed, each with its architecture and process.

Named Data Networking (NDN)[24] is an ICN approach that utilizes named data to provide communication services. NDN replaces IP addresses with content names, which enables efficient content delivery and reduces the complexity of the network architecture. In NDN, data is cached throughout the network, which results in faster and more efficient content delivery.

Content-Centric Networking (CCN)[25] is another ICN approach that prioritizes content over hosts or locations. CCN uses content names as a means of addressing content, and content routers in the network handle the task of forwarding the content. CCN is designed to handle high traffic loads and can easily scale to accommodate large networks.

The PURSUIT (Publish-Subscribe Internet Technology)[30] approach focuses on providing secure and efficient communication using public-key encryption techniques. PURSUIT employs a publish-subscribe model, where publishers can publish content, and subscribers can receive the content. PURSUIT utilizes cryptographic techniques to ensure secure content delivery.

MobilityFirst[26] is an ICN approach that focuses on providing seamless mobility for end-users across various network architectures. Mobility First provides a mobile-IP-like service that allows users to move seamlessly among networks without losing connectivity. Mobility First also provides security features that ensure secure data transfer between devices.

CONVERGENCE[3] is an ICN approach that aims to integrate various communication networks to provide more efficient and seamless communication. CONVERGENCE utilizes the publish-subscribe model and content-based routing to ensure efficient content delivery. CONVERGENCE also provides seamless mobility and security features that make it ideal for use in large-scale networks.

NetInf (Network of Information)[29} is an ICN approach that prioritizes content-based addressing for efficient data transfer. In NetInf, data is stored and transferred based on content names, which ensures that the most suitable source is always utilized. NetInf also provides caching features that ensure fast and efficient content delivery.

Finally, the Data Oriented Network Architecture (DONA)[28] approach is centered on providing more efficient and secure data transfer by utilizing unique object identifiers instead of host or location-based identifiers. DONA employs a publish-subscribe model, where publishers can publish data, and subscribers can receive the data. DONA provides a secure communication channel that ensures secure data transfer between devices.

In conclusion, ICN provides a more efficient and scalable network architecture that prioritizes content over hosts or locations. The various ICN approaches, including NDN, CCN, PURSUIT, Mobility First, CONVERGENCE, NetInf, and DONA, each offer unique features that make them ideal for use in different network architectures.

IV. ICN Key Features

ICN was originally proposed as a groundbreaking network paradigm for accessing named data objects, with the potential to transform the architecture of the Internet. The direct accessibility of data objects facilitates more efficient and widespread in-network caching, replication, and data dissemination, leading to improved utilization of network bandwidth and enhanced scalability. However, realizing these advantages requires addressing various technological challenges within the ICN framework. These include establishing unique identification mechanisms for named data objects, developing efficient mechanisms for discovering and delivering named data objects to clients, ensuring the security of widely distributed named data objects across the network, and enabling mobility in an information-centric and location-independent manner. Solving these research problems is crucial to harnessing the full potential of ICN.

Naming: Using names to identify data objects regardless of location[31] is critical for ICN. There are two main methods in ICN for uniquely naming data objects: flat naming scheme and hierarchical naming scheme. It is feasible to aggregate routing data and increase a routing scheme's scalability with the former, which is based on a publisher's prefix. In contrast, the latter makes use of a data object's hash value, such as its name or content. The flat naming method uses a hashing scheme to provide a fixed length name for each data object, which reduces the time it takes to perform reputation lookups.

Routing and forwarding: Name resolution, discovery, and delivery are the three main ICN routing operations. The process of name resolution consists of transforming a data object's name into its locator. Finding the location of the requested data object is the responsibility of the discovery process. The required data item is finally sent to the client during the delivery step. Route by name routing (RBNR) and lookup by name routing (LBNR) are the two basic categories under which ICN routing can be divided. With RBNR, the name of the data object serves as the basis for the router's decision regarding the best course of action in a single step that combines the name resolution and discovery phases. On the other hand, LBNR separates the name resolution and discovery phases into two distinct steps, where the router first determines the location of the data object through name resolution and then discovers the optimal path to the data object.

Caching: ICN Mobility aims to provide seamless and uninterrupted content delivery to clients in ICN applications, even if their physical location changes. This is achieved through receiver-driven content retrieval, where clients request content and receive it continuously without any noticeable disruptions. The challenge is in offering server-side mobility, though. ICN Mobility must cooperate closely with ICN routing in order to guarantee that the same data object is located during a transfer.

Security and privacy: ICN's in-network cache allows data items to be retrieved from anywhere in the network, but this raises concerns about the trustworthiness of the data's origin. To solve this problem, ICN needs a security system to guarantee that the retrieved data hasn't been altered since it was published legally. Data object and publisher consistency is checked as part of data origin authentication, which is a crucial component of ICN security. Without these safety precautions, the network is open to a number of attacks, such as DoS attacks that inject harmful content into the network. Therefore, ensuring the security and authenticity of ICN data is crucial for maintaining the integrity and reliability of the network.

Table 2 : Comparison of Properties of Various ICN Architectures

ICN Architecture **Properties**	**Content-Centric Networking (CCN)**	**Named Data Networking (NDN)**	**DONA (Data-Oriented Network Architecture)**	**Mobility First**	**Netinf**	**CONVERGENCE**	**PURSUIT**
Content/ Object Model	Named Data Objects (NDOs)	Named Data Objects (NDOs)	Handles	Mobile Named Data (MND)	Named Information Objects (NIOs)	Named Information Objects (NIOs)	Named Information Objects (NIOs)

Routing	Hop-by-hop forwarding	Longest Prefix Matching	Hierarchical	Identifier-Locator Separation	Flat routing	Interest-based routing	Query-based routing
Security	Trust Management	Signature-Based	Name-Based	Name-Based	Digital signatures	Trust management	Cryptographic security
Caching	In-network caching	In-network caching	Distributed caching	Caching at various levels	Content caching	Caching at various levels	Content caching
Name Resolution	Interest-Data exchange	Interest-Data exchange	Globally unique names	Hierarchical and flat names	Dynamic name resolution	Name-based resolution	Content-based resolution
Scalability	Hierarchical structure	Scalable forwarding plane	Scalable forwarding plane	Scalable forwarding plane	Scalable architecture	Scalable architecture	Scalable architecture
Mobility Support	Supports mobility	Supports mobility	Mobility management and routing	Designed for mobility	Supports mobility	Supports mobility	Mobility management
QoS Support	QoS-aware forwarding	QoS-aware forwarding	QoS-aware forwarding	QoS-aware forwarding	QoS-aware forwarding	QoS-aware forwarding	QoS-aware forwarding
Routing Protocol	Distance Vector	Link State	Distance Vector	Hierarchical routing	Distance Vector routing	Interest-based routing protocol	Query-based routing protocol
Interest/ Data Processing	In-network processing	In-network processing	In-network processing	In-network processing	In-network processing	In-network processing	In-network processing

V. Security Attacks in ICN

Multiple security issues must be resolved by ICN. ICN contains new forms of attacks that have not been seen before or have not had a significant impact on previous environments. ICN circumstances can also occur in a range of episodes that take place in various contexts. The four categories of ICN attacks[32] (including new and traditional attacks) are as follows: naming, routing, caching, and other assaults. This classification is determined by the attacker's main objective. Every episode only focuses on one topic; however it might have an effect on other categories as well.

ICN routing and caching are impacted, for example, by flooding and unpopular request assaults. The fundamental goal of a flooding assault is to overwhelm and deplete the routing resources, which affects the caching system. Unpopular request attacks primarily aim to violate cache relevance, which impacts the routing mechanism. The following four paragraphs provide a brief introduction to the suggested categories.

Security Attacks and Counter measures

Attacks on Naming: ICN infrastructures pose a more significant risk to user privacy. Many attackers attempt to censor or track online activity. With greater access to user requests made possible by an ICN design, attackers will have control over the flow of information and would find it much easier to prevent it. In attacks on ICN involving names, the attacker attempts to halt the dissemination of a certain piece of content by halting delivery and identifying the request's source.

- Watchlist: This type of attack is known as content filtering or censorship in ICN. It involves selectively blocking or removing content based on certain criteria such as keywords, origin, or content type. The attacker can do this by monitoring network traffic and examining packet payloads to identify specific content names that they want to filter or remove. This can be accomplished by modifying or dropping packets that match the attacker's predefined criteria. Use of encryption to shield the data from unauthorized readers is one technique to lessen the impact of this kind of assault. Another approach is to use obfuscation techniques to hide the content's name or metadata, making it difficult for the attacker to identify and filter the content. Additionally, network-level solutions such as traffic analysis and anomaly detection can help detect and mitigate content filtering attacks.
- Sniffing:The sniffing attack differs from the watchlist attack by continuously scanning the network for content that may need filtering or removal. Unlike the watchlist attack, which relies on a predetermined list, the sniffing attacker dynamically analyses requests or content to determine if supplied keywords are present. Although both attacks share similarities in their scenarios, the distinguishing factor is the attacker's reliance on real-time analysis rather than a pre-existing list.

Attacks on Routing: Attacks on routing aim to disrupt or compromise the routing mechanisms and processes within the ICN infrastructure. These attacks have notable implications on the efficient and secure delivery of content in ICN networks. Common attacks on routing in ICN are:

- Infrastructure Attacks: Infrastructure attacks aim to disrupt or compromise the underlying routing infrastructure in ICN.Examples include attacks on routers, switches, or other network devices that handle the routing of content in ICN.These attacks can lead to the degradation or complete disruption of routing services, impacting the delivery of content.

- Source Attacks: Source attacks involve compromising the source of content in ICN.Attackers may impersonate legitimate content sources or inject malicious content into the network.These attacks can result in the dissemination of incorrect or malicious content, leading to information manipulation or unauthorized access.
- Mobile Blocking Attacks: Mobile blocking attacks target the mobility aspects of ICN and aim to disrupt the movement of content and nodes.Attackers may attempt to block or hinder the routing of content to mobile devices or disrupt the handover process between different network access points.These attacks can lead to service interruptions, delays in content delivery, or the denial of access to mobile users.
- Timing Analysis Attacks[27]: Timing analysis attacks involve monitoring and analyzing the timing patterns of network responses to gain insights into the network's behavior. Attackers can observe the time taken for a content request to traverse the network, the time it takes to receive a response, or the timing of other network events. By analyzing these timing patterns, attackers can potentially infer information about the network's topology, content popularity, or even identify specific nodes or routes.
- Flooding and Jamming Attacks: Flooding and jamming attacks involve overwhelming the ICN network with a high volume of traffic or interference.Attackers may flood the network with excessive content requests, causing congestion and affecting the normal routing of content. Jamming attacks can disrupt the wireless communication channels used in ICN, making it difficult for nodes to communicate and exchange content.
- Hijacking Attacks: Hijacking attacks in ICN involve the unauthorized control or manipulation of content routing paths.Attackers may hijack the routing paths of content, diverting it to unintended destinations or intercepting and modifying it.These attacks can lead to data interception, unauthorized access to content, or the injection of malicious content into the network.
- Interception Attacks: Interception attacks focus on intercepting and eavesdropping on content transmissions in ICN.Attackers may attempt to capture and analyze content packets to extract sensitive information or gather intelligence.These attacks can compromise the confidentiality and privacy of content, potentially exposing sensitive data to unauthorized parties.

Attacks on Caching: Attacks on caching in Information-Centric Networking (ICN) aim to exploit vulnerabilities in the caching mechanisms and processes within the ICN infrastructure. By compromising the caching system, attackers can manipulate or disrupt the efficient storage and retrieval of content in ICN networks. Common attacks on caching in ICN are:

- Cache Poisoning: Attackers attempt to insert malicious or invalid content into the ICN caches. By injecting false content or manipulating the metadata associated with cached objects, they can deceive users or corrupt the cached data.

- Cache Flooding: This attack involves overwhelming the caches with a large volume of requests or unnecessary content. By flooding the caches, attackers can exhaust the available storage space, degrade the caching performance, and impede the delivery of legitimate content.

- Cache Pollution: In cache pollution attacks, attackers deliberately request popular or frequently accessed content that they have no genuine interest in. This strategy aims to fill the caches with irrelevant content, making it more challenging for legitimate users to retrieve the desired data efficiently.
- Cache Timing Attacks: These attacks exploit the timing patterns or characteristics of cache updates or evictions to gain insights into the popularity or availability of specific content. By analyzing the timing information, attackers may deduce sensitive information, such as user behavior or content popularity, potentially compromising privacy or impacting the efficiency of content delivery.
- Cache Replay Attacks: Attackers capture and replay previously cached content to deceive users or disrupt the delivery of fresh content. By replaying stale or outdated content, they can manipulate the perception of content availability or integrity.

  To mitigate attacks on caching in ICN, several security measures can be implemented. These include secure content signing and verification mechanisms, access control policies for cache updates, detection and prevention of cache poisoning attacks through integrity checks, rate limiting to mitigate cache flooding, monitoring and analysis of caching behavior to identify anomalies, and encryption of cached content to protect its confidentiality. Additionally, user education and awareness play a crucial role in mitigating the impact of caching attacks by promoting safe content consumption practices.

• **Miscellaneous Attacks:** The objective of these attacks[32] is to disrupt ICN services and gain unauthorized access. As a consequence, these assaults lead to the transmission of incomplete or erroneous data.

- Mistreatment of packets: They are prevalent active network attacks that take place during data transmission, with a focus on replay attacks. Attackers who gain unauthorized access to links, either through deception or malicious intent, often engage in actions aimed at blocking, modifying, or tampering with requested content. In the described attack scenario, the attacker gains access to ICN nodes or network links and performs activities such as packet manipulation. They operate concurrently by transmitting data, frequently responding to inquiries, or generating content on behalf of legitimate users.
- Misusing the signer's secret: An attacker can exploit various common attacks to gain unauthorized access to the signer's keys. In the context of ICN, this issue holds significant importance as publishers sign contracts for widely and continuously accessible materials. These contracts typically contain public information along with the publisher's signature. Due to the large volume of this data, it becomes comparatively easier for the attacker to acquire the signer's key.

- Unauthorized entry: Unauthorized access attacks allow an attacker to view content that is intended for specific users or groups, even without proper permission. In the case of ICN, where content is distributed across multiple network locations, these attacks take advantage of any readily accessible copies, making them relatively easier to execute.

VI. Security Challenges

Each challenge's research difficulty is first described in great depth to provide readers with a better understanding of how it differs from typical IP network strategies. Each challenge concludes with a summary of research issues for good ICN research subjects. It talks about the research problems that need to be solved to support ICN applications.

- **Data Protection (Confidentiality and Integrity):** Information Centric Networking (ICN) provides several advantages over traditional networking approaches, such as efficient content delivery, seamless mobility, and scalability. However, ICN also presents unique security challenges that must be addressed to ensure secure data transfer. One of the primary security challenges in ICN is data protection, which includes confidentiality and integrity. Since ICN is a content-centric approach, data is retrieved based on content names, which increases the risk of data interception and unauthorized access. To address this challenge, ICN approaches utilize encryption techniques, such as public-key cryptography, to ensure secure content delivery. Additionally, data integrity is maintained by utilizing cryptographic hash functions to ensure that data is not tampered with during transfer. However, as ICN continues to evolve, new security challenges may emerge, and it will be crucial to continually evaluate and update security measures to ensure the integrity and confidentiality of data transferred over ICN.
- **Routing Security:** In Information Centric Networking (ICN), routing security[20] is another significant challenge that should be addressed to ensure secure data transfer. Since ICN uses content-based routing, the routers in the network must ensure that the content is forwarded to the correct destination. However, this approach increases the risk of routing attacks, where an attacker can intercept and modify the routing information to redirect traffic to a malicious destination. To address this challenge, ICN approaches employ various security measures, such as cryptographic signatures, to ensure that routing information is authentic and has not been tampered with. Additionally, ICN approaches utilize secure routing protocols, such as Trust Anchor Group (TAG), to ensure that only authorized routers can participate in the routing process. Despite these measures, routing security remains a significant challenge in ICN, and it will be crucial to continue to evaluate and update security measures to ensure secure and reliable routing of data in ICN networks.
- **Content Caching:** Content caching is a fundamental aspect of Information Centric Networking (ICN) that enables faster and more efficient content delivery by storing frequently accessed content at the network edge. However, content caching in ICN also presents unique security challenges that must be addressed to ensure secure data transfer. One significant challenge is the risk of cache poisoning attacks[20], where an

attacker can modify the content stored in the cache to redirect traffic to a malicious destination. To address this challenge, ICN approaches employ various security measures, such as cryptographic signatures and content validation, to ensure that the cached content is authentic and has not been tampered with. Additionally, ICN approaches utilize secure cache management protocols, such as Cache Access Protocol (CAP), to ensure that only authorized entities can access and modify the content in the cache. Despite these measures, content caching security remains a significant challenge in ICN, and it will be crucial to continue to evaluate and update security measures to ensure secure and reliable content caching in ICN networks.

- **Security of Named Data Objects (NDO's):** In Information Centric Networking (ICN), Named Data Objects (NDOs) are the fundamental building blocks of data exchange, representing data as a named entity that can be accessed directly by name rather than by its physical location. However, the security of NDOs presents unique challenges that must be addressed to ensure secure data transfer. One significant challenge is the risk of data tampering, where an attacker can modify the content of the NDO to inject malicious code or redirect traffic to a malicious destination. To address this challenge, ICN approaches employ various security measures, such as digital signatures and hash functions, to ensure that NDOs are authentic and have not been tampered with. Additionally, access control mechanisms, such as Access Control Lists (ACLs) and Key Management Systems (KMSs), are used to ensure that only authorized entities can access and modify the NDOs. Despite these measures, the security of NDOs remains a significant challenge in ICN, and it will be crucial to continue to evaluate and update security measures to ensure secure and reliable exchange of NDOs in ICN networks.
- **Access control:** Creating scalable object-based access control techniques is another challenge specific to ICN. Access to sensitive network data has previously been protected using several encryption approaches [20]. Numerous design strategies exist above the network layer, especially in CCN and NDN [21]. Publish-subscribe ICNs, like ENCODERS [22], on the other hand, incorporate access control into the network layer. It takes advantage of multi-authority attribute-based encryption [23] to restrict content access to particular system nodes. Peers act as brokers to match content from publishers with subscriber interests because the system is decentralized. In this instance, reachability limits that are separate from those established by the routing protocols are essentially created.
- **User Privacy:** In ICN-based architectures, privacy has always been elusive. The content payloads, signatures, and even the names of packets can reveal a lot of information about designs. The privacy of terms was one of the main topics of discussion at this conference. Name privacy, as used in this context, is the quality that no relationship or correlation exists between a so-called "network name," or the name encoded in a packet, and the accompanying content item. Name privacy means explicitly that nothing about the data contained in the content object may be inferred from the network name. Names should give no more information than an IP address and port already do. It is more complex to add name privacy to ICN-based architectures. Think about how this would operate if it were executed cleanly, that is, without utilizing

any upper-layer services. One may make the following assumptions to limit the design space:

a) The identification (ID) of a piece of material, such as its cryptographic hash digest, may ask for the piece of content. The protection of privacy is not compromised by revealing the content ID, either.
b) The public key of the producer is known by the consumers, and they desire to share it. Routable prefixes and application-specific suffixes are inherent in network names. Customers are unaware of the location and identifier split in a name by default.
c) When making requests in an ICN network, consumers can include various pieces of information, such as details about the expected content, a signature verification key, or an ID. Based on these assumptions, there are two primary methods for issuing a request: (1) with a content ID and (2) without a content ID. These approaches have different implications for the network's caching and routing systems, as requests with content IDs are more likely to be matched with cached copies in the network. This can lead to more efficient and faster content delivery. However, requests without content IDs may be necessary in certain cases, such as when the ID is unknown or when the content is dynamic and changes frequently. ICN networks must be designed to support both types of requests and provide robust security measures to protect against unauthorized access to content.

A request name must have a routable prefix to route it to a cache or producer that can deliver the required content. This strategy can achieve our goal of name privacy because these locators can be kept apart from the desired material. To get the requested content without explicit location information, a higher-layer service is necessary.

A name's application-specific suffix must not give away any information about the contents. Encrypting a payload's name and content in a communication system raises various challenges and considerations. Obtaining the routable prefix can be addressed by having a central authority that manages the prefixes or by using a distributed system like a blockchain. The choice of encryption key is critical and should ensure that the key is secure and not susceptible to hacking. Even if the finished product isn't encrypted, the content response needs to be to safeguard the outcome. Using the producer's public key to encrypt the name suffix is one option.

- **Key Management**: Key management[33] is a critical aspect of Information Centric Networking (ICN) that ensures the secure exchange of data by enabling the distribution and management of cryptographic keys used to encrypt and decrypt data. However, key management in ICN presents unique security challenges that must be addressed to ensure secure data transfer. One significant challenge is the risk of key compromise, where an attacker can intercept and obtain the keys used to encrypt and decrypt data, allowing them to access and modify the data. To address this challenge, ICN approaches utilize various security measures, such as secure key exchange protocols and key revocation mechanisms, to ensure that only authorized entities have access to the keys. Additionally, ICN approaches use secure key storage techniques, such as Hardware Security Modules (HSMs) and Secure Enclaves, to protect the keys from unauthorized access. Despite these measures, key management security remains a significant challenge in ICN, and it will be crucial to continue to evaluate and update security measures to ensure secure and reliable key management in ICN networks.

- **Trust Management:** Trust management[34] plays a vital role in securing data transfer within Information Centric Networking (ICN) by allowing the assessment and control of network entities' trustworthiness. However, trust management in ICN comes with its own set of unique security challenges that need to be addressed to ensure safe data transfer. A significant issue is the potential for trust exploitation, where attackers can compromise the trust evaluation process to gain unauthorized access to the network or manipulate data transfer. To mitigate this risk, ICN approaches employ several security measures such as secure trust evaluation mechanisms, trust revocation protocols, and secure trust storage techniques like Trusted Platform Modules (TPMs) and Secure Elements to safeguard the trust evaluation process. Despite these measures, trust management security remains a significant challenge in ICN, requiring continued evaluation and updates to ensure dependable and secure trust management in ICN networks.

VII. SECURITY PROPERTIES OF DIFFERENT ARCHITECTURES:

(i) AVAILABILITY

NDN:

NDN has strong support for availability. Due to the Forwarding Information Base, all interest packets sooner or later reach the node that has the requested data if the packet has a valid name for the data. Nodes on the path of the response can cache the data in the Content Store, thus allowing for even greater availability in case of big network latency or if the original producer is not available at the moment. Additionally, Denial of Service attacks such as Interest Flooding which hinder availability the most can be mitigated by monitoring the Pending Interest

PURSUIT

Given a valid content name - a pair of scope ID and rendezvous ID, Rendezvous Nodes, Forwarding Nodes, and Topology Manager always find a way to deliver the requested content if such a way exists. Therefore, availability is supported by the PURSUIT

NetInf

NetInf allows for hybrid forwarding - supporting both Name Resolution Service and name-based routing. This allows for better flexibility for GET request forwarding. Also, NetInf can use both on-path and off-path caching, thus improving data availability even more. Given all that, NetInf has good support for availability.

(ii) ACCESS CONTROL:

NDN:

As stated earlier and explained by Zhang et al, NDN supports name-based access control through encryption [24]. NDN employs a model similar to Simple Distributed Security Infrastructure (SDSI/SPKI) for managing keys. It uses hierarchical namespaces and predefined key name generation procedures so that both consumers and producers can easily reach the same name for the data that holds the key. Thus, it is easy to encrypt the data and provide the decryption keys only to the authorized consumers.

PURSUIT

Data in the response packets can be encrypted, restricting access to the data to only those users who have the encryption key. Thus, PURSUIT supports access control.

NetInf

Similar to NDN and PURSUIT, NetInf can employ symmetric encryption in order to provide access control for requested data.

(iii) Data Integrity

NDN

NDN does not have explicit support for data integrity, however, it can be achieved by attaching a digest of the message to the message itself. This way upon receiving a message client can recompute its digest and compare it with the received digest. If they match, then the message has not been tampered with.

PURSUIT

PURSUIT inherits Packet Level Authentication (PLA) with per-packet signatures from its predecessor In addition to other features, these signatures provide data integrity verification [12]. Hence, PURSUIT supports data integrity.

NetInf

The CLs of NetInf provide message integrity and validate the integrity of all received messages before possibly assembling the whole message and sending it to the higher layer in the network stack. This is achieved by providing a SHA-256 hash in the application-specific metadata inside the NDO. Therefore, NetInf supports message integrity.

(iv) Nonrepudiation

NDN

As stated earlier, the Interest packets in NDN carry the signature constructed from the producer's private key. It can be found in the Data packet field called publisher ID. Thus, the producer cannot later repudiate that he/she produced this data.

PURSUIT

Per packet signatures in PLA provided by PURSUIT allow for nonrepudiation on the network layer by using elliptic curve cryptography. Hence, PURSUIT supports nonrepudiation.

NetInf

NetInf does not have built-in support for nonrepudiation, but it can be achieved by attaching a signature of the producer's private key or providing a signature in a separate data packet. Similar to hash stored in the application-specific metadata inside the NDO, signature can also be provided in a similar manner.

(v) Data authentication

NDN

NDN supports both data integrity and data origin validations, therefore data authentication is supported. A signature of the producer's private key and digest of the produced data are enough to verify that the data was produced by the expected producer and has not been tampered with. Signature and publisher ID along with needed metadata such as digest algorithm are all provided in every Data packet [23]. Hence, NDN supports data authentication.

PURSUIT As stated by Lagutin et al, PURSUIT's per packet cryptographic signatures provide data authentication on the network layer using elliptic curve cryptography (ECC). ECC provides a good security with small key sizes which means that the key can easily be included in every packet [12]. Thus, data authentication is supported in PURSUIT.

NetInf

NetInf has built-in support for data integrity, but it does not explicitly support the data origin authentication. It can support data origin authentication by attaching a signature of the producer’s private key. Thus, NetInf does not have full support for data authentication, but it can if data origin authentication is supported.

Table 3 : Security Properties of Various ICN Architecture

Security Property	NDN	CCN	MobilityFirst	Netinf	PURSUIT
Availability	Built-in Interest Flooding, Caching Mechanisms	Built-in Interest Flooding, Caching Mechanisms	Resilient to Network disruptions	Availability is dependent on individual node availability	Resilient to Network disruptions
Access Control	Access Control Lists (ACLs)	Access Control Lists (ACLs)	Access Control Lists (ACLs)	Access Control Lists (ACLs)	Access Control Lists (ACLs)
Data Integrity	Signature-Based Cryptography	Signature-Based Cryptography	Forward Secrecy Cryptography	Digital Signatures	Access Control & Encryption
Data Authentication	Signature-Based Cryptography	Signature-Based Cryptography	Forward Secrecy Cryptography	Digital Signatures	Access Control & Encryption
Non-Repudiation	Public-Key Cryptography	Public-Key Cryptography	Public-Key Cryptography	Public-Key Cryptography	Access Control & Encryption

VIII Conclusion

In Conclusion, Information Centric Networking (ICN) offers a promising solution for addressing the challenges associated with content distribution and mobility in edge computing. ICN's features, including location-independent naming, in-network caching, name-based routing, and data self-security, provide efficient and scalable content distribution without relying on host-centric network architecture. Despite its potential benefits, ICN also presents distinctive security challenges that Should be addressed to guarantee secure and reliable data transfer. These security challenges include data protection, routing security, content caching security, security of Named Data Objects (NDO's), key management security, and trust management security. Therefore, continued research and development is needed in providing security to ICN is essential to ensure its successful adoption and implementation in modern networks.

References

[1] Nour, B., Sharif, K., Li, F., Biswas, S., Moungla, H., Guizani, M., & Wang, Y. (2019). A survey of Internet of Things communication using ICN: A use case perspective. *Computer Communications*, 142, 95-123.

[2] Aldaoud, M., Al-Abri, D., Awadalla, M., & Kausar, F. (2023). Leveraging ICN and SDN for Future Internet Architecture: A Survey. *Electronics*, 12(7), 1723.

[3] Xylomenos, G., Ververidis, C. N., Siris, V. A., Fotiou, N., Tsilopoulos, C., Vasilakos, X., ... &Polyzos, G. C. (2013). A survey of information-centric networking research. *IEEE communications surveys & tutorials*, 16(2), 1024-1049.

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

[5] C. Tsilopoulos and G. Xylomenos, "Supporting diverse traffic types in information centric networks," *in Proc. of ACM SIGCOMM workshop on Information-centric networking*, ser. ICN '11. New York, NY, USA: ACM, 2011, pp. 13–18.

[6] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest flooding attack and countermeasures in named data networking," *in Proc. of IFIP Networking Conference*, Brooklyn, NY, USA, 2013, pp. 1–9.

[7] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "DoS and DDoS in named data networking," *in Proc. of 22nd ICCCN, Nassau, Bahamas*, 2013, pp. 1–7.

[8] L. Yao, Y. Zeng, X. Wang, A. Chen, and G. Wu, "Detection and defense of cache pollution based on popularity prediction in named data networking," *IEEE TDSC*, pp. 1–1, 2020.

[9] H. Salah, M. Alfatafta, S. SayedAhmed, and T. Strufe, "CoMon++: Preventing cache pollution in NDN efficiently and effectively," *in Proc. of 42nd IEEE LCN. Singapore: IEEE*, 2017, pp. 43–51.

[10] A. Karami and M. Guerrero-Zapata, "An ANFIS-based cache replacement method for mitigating cache pollution attacks in named data networking," *Computer Networks*, vol. 80, pp. 51–65, 2015.

[11] T. Nguyen, H. Mai, G. Doyen, R. Cogranne, W. Mallouli, E. M. d. Oca, and O. Festor, "A security monitoring plane for named data networking deployment," *IEEE Communications Magazine*, vol. 56, no. 11, pp. 88– 94, 2018.

[12] P. Tammana, R. Agarwal, and M. Lee, "Distributed network monitoring and debugging with SwitchPointer," *in 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18). Renton, WA: USENIX Association*, Apr. 2018, pp. 453–456.

[13] P.-W. Tsai, C.-W. Tsai, C.-W. Hsu, and C.-S. Yang, "Network Monitoring in Software-Defined Networking: A Review," *IEEE Systems Journal*, vol. 12, no. 4, pp. 3958–3969, Dec. 2018.

[14] T. Nguyen, X. Marchal, G. Doyen, T. Cholez, and R. Cogranne, "Content poisoning in named data networking: Comprehensive characterization of real deployment," *in Proc. of IFIP/IEEE IM, Lisbon, Portugal*, 2017, pp. 72–80.

[15] S. Lee, K. Levanti, and H. S. Kim, “Network monitoring: Present and future,” *Computer Networks*, vol. 65, pp. 84–98, Jun. 2014.

[16] H. C. A. van Tilborg and S. Jajodia, Eds*., ISO 15408 CC – Common Criteria. Boston, MA: Springer US*, 2011, pp. 648–648.

[17] M. Anisetti, C. A. Ardagna, E. Damiani, and F. Gaudenzi, “A semiautomatic and trustworthy scheme for continuous cloud service certification,” *IEEE TSC*, vol. 13, no. 1, pp. 30–43, 2020.

[18] M. Anisetti, C. Ardagna, E. Damiani, and G. Polegri, “Test-Based Security Certification of Composite Services,” *ACM Transactions on the Web*, vol. 13, no. 1, pp. 3:1–3:43, Dec. 2018.

[19] Yu, K., Eum, S., Kurita, T., Hua, Q., Sato, T., Nakazato, H., ... &Kafle, V. P. (2019). Information-centric networking: Research and standardization status. *IEEE access*, 7, 126164-126176.

[20] R. Tourani, T. Mick, S. Misra, and G. Panwar, “Security, privacy, and access control in information-centric networking: A survey,” *arXiv preprint arXiv:1603.03409*, 2016.

[21] C. Ghali, M. A. Schlosberg, G. Tsudik, and C. A. Wood, “Interest-based access control for content centric networks,” *in International Conference on Information-Centric Networking. ACM*, 2015.

[22] M. Raykova, H. Lakhani, H. Kazmi, and A. Gehani, “Decentralized authorization and privacy-enhanced routing for information-centric networks,” *in Proceedings of the 31st Annual Computer Security Applications Conference. ACM*, 2015, pp. 31–40.

[23] M. Chase, “Multi-authority attribute based encryption,” *in Theory of Cryptography Conference. Springer*, 2007, pp. 515–534.

[24] NSF Named Data Networking project [online] Available https://named-data.net/project/

[25] Athanasios V. Vasilakos, Zhe Li, Gwendal Simon, Wei You “Information centric network: Research challenges and opportunities” Journal of Network and Computer Applications 52(2015)1–10

[26] MobilityFirst project [online] Available https://mobilityfirst.cs.umass.edu/

[27] Aziz Mohaisen, Hesham Mekky, Xinwen Zhang, Haiyong Xie, Yongdae Kim “Timing Attacks on Access privacy in Information Centric Networks” IEEE Transactions on Dependable and Secure Computing, VOL. 1, NO. 8, AUGUST 2014

[28] Teemu Koponen, Mohit Chawla, Byung-Gon Chun, Andrey Ermolinskiy “A Data Oriented(and beyond) Network Architecture” *SIGCOMM’07*, August 27–31, 2007, Kyoto, Japan.

[29} Christian Dannewitz, Dirk Kutscher, Börje Ohlman, Stephen Farrell, Bengt Ahlgren, Holger Karl,Network of Information (NetInf) – An information-centric networking architecture,Computer Communications,Volume 36, Issue 7,2013 Pages 721-735,ISSN 0140-3664

[30] PURSUIT project [online] Available https://cordis.europa.eu/project/id/257217

[31] S. S. Adhatarao, J. Chen, M. Arumaithurai, X. Fu and K. K. Ramakrishnan, "Comparison of naming schema in ICN," *2016 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)*, Rome, Italy, 2016, pp. 1-6, doi: 10.1109/LANMAN.2016.7548856.

[32] Eslam G. AbdAllah, Hossam S. Hassanein, Mohammad Zulkernine “A Survey of Security Attacks in Information-Centric Networking” 10.1109/COMST.2015.2392629, IEEE Communications Surveys & Tutorials

[33] Bander A Alzahrani, Vassilios G. Vassilakis and Martin J. Reed “Key Management in Information Centric Networking”, International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.6, November 2013.

[34] Geetanjali Rathee , Ashutosh Sharma, Rajiv Kumar , Farhan Ahmad , Razi Iqbal “A trust management scheme to secure mobile information centric networks”, Computer Communications 151 (2020) 66–75.