IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 16 November 2022, accepted 9 January 2023, date of publication 23 January 2023, date of current version 26 January 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3238732

SURVEY

Security and Integrity Attacks in Named Data Networking: A Survey

MOHAMMAD SHAHRUL MOHD SHAH[1], YU-BENG LEAU[1], (Senior Member, IEEE), MOHAMMED ANBAR[2], (Member, IEEE), AND ALI ABDULQADER BIN-SALEM[3]

[1]Faculty of Computing and Informatics, Universiti Malaysia Sabah, Kota Kinabalu 88400, Malaysia
[2]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, George Town, Penang 11800, Malaysia
[3]School of Computer Science and Technology, Zhoukou Normal University, Zhoukou 466001, China

Corresponding author: Yu-Beng Leau (lybeng@ums.edu.my)

This work was supported by the Ministry of Higher Education Malaysia for Fundamental Research Grant Scheme under Grant FRGS/1/2019/ICT03/UMS/02/2.

ABSTRACT The notion of Information-Centric Networking (ICN) specifies a new communication model that emphasis on the content exchanged rather than the devices connected. ICN architectures like Content Centric Network (CCN) and Named Data Networking (NDN) have been proposed to shift from host-centric based to content-centric based communication along and provide benefits to users in addressing the challenges of traditional IP networks. It differs from host-centric standard Internet Protocol (IP) networking in of naming, routing, forwarding, and caching characteristics. Naming features used in NDN use global unique names provided by content-based security and encryption. It ensures content integrity and authenticity as part of its design. In this paper, we survey on security aspects of NDN/CCN, discussing three integrity attacks such as replay attacks, Man-in-The-Middle (MiTM) attacks, and Content Poisoning Attack (CPA) with countermeasure against them. In addition, we highlight an open challenge and offer future research directions in the context of security.

INDEX TERMS Information-centric networking, named data networking, content poisoning attack, content integrity, access control, blockchain.

I. INTRODUCTION

As we move forward and made a great stride in terms of how we communicate, the design of the technology changed the way the data is distributed between computers. One of the most significant impacts of the Internet on digital communication is that it dramatically diminishes the importance of geographical location in how individuals interact. Currently, the Internet is constructed on a host-centric based architecture, which leads to an increase in a number of connected devices and content development, both of which are essential for obtaining and exchanging data. The Internet has a wide range of applications, and it has recently become a source for multimedia content. In the 1970s, the Transmission Control Protocol and the Internet Protocol that we recognize today as TCP/IP were developed that allowed for point-to-point communication via the internet [1]. The fundamental idea is to let one of the hosts to deliver data packets to another host by making use of its IP address. On the other hand, the current application communication paradigm has moved away from the practice of delivering content to the end-host and now focuses on retrieving content from wherever it is available. The process of accessing content is more significant than addressing hosts. For instance, to facilitate access to this type of content, a Content Distribution Network (CDN) [2] has been developed on top of the TCP/IP protocol.

Peer-to-Peer (P2P) [3] and CDN [4] act as an overlay network that serves the content to end-users that allows computer to communicate. The idea behind peer-to-peer networking is that data can be exchanged directly between any two stations that are linked to the same network, bypassing the need for a central server. It grants the capability to all workstations to behave directly in the roles of client

The associate editor coordinating the review of this manuscript and approving it for publication was Fung Po Tso.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

and server. Nonetheless, decentralized peer-to-peer systems have greater challenges than client-server systems have been doing in spreading data and delivering the interconnection of nodes, which is necessary for assuring minimal delays in requests. As CDN compared to NDN [5], the Internet has shifted from means of communication to content distribution. According to the Cisco Annual Internet Report [6], there will be 29.3 billion networked devices by 2021 from 18.4 billion in 2018. In TCP/IP, content security is achieved by securing the channel between end-points and with high traffic, it would lead to scalability and manageability issues. Incompatibility between design used shows IP architectural limitations, motivating researchers to find innovative solutions. The most significant drawback is associated with the total cost that is incurred where CDN is extremely costly options, particularly when being implemented on a massive scale. Demonstrating the benefits that they offer, CDN and P2P networks does not provide a game-changing answer to the underlying issues that caused by the existing architecture of the internet. For this reason, a significant amount of work has been put together over the course of the past few years to establish clean-slate approaches for the structure of the future Internet.

The current architecture of the Internet was meant to be a means of connecting pairs of hosts and to enable these hosts to exchange packets in a reliable manner. The way we use it on a daily basis has shifted drastically from simple communication to the distribution of content. The Information Centric Networking (ICN) [7], [8], [9] is a new paradigm emerged as a result of an effort to start the process of designing the future internet architecture from a clean-slate. As ICN focuses on the efficient and scalable distribution of content to meet the requirements of 21st-century Internet usage that is being considered for the architecture of the future internet, in which content-based communication does not take into account the device's physical address. The communication model that shifted from the traditional host-centric-based model to the content-centric-based model that specifies content names instead of location benefits inherent content integrity [10]. The terminology in ICN consists of three main terms: Named Data Objects (NDO), publisher, and requestor [11]. Content in ICN is uniquely identified by location-independent names, with the goals of efficient NDO dissemination and retrieval on a global scale. There will be a need to address the collecting data process to be more efficient and less time consuming to manage, and this aligned with ICN goals to provide users with a better perspective of what could have been accomplished.

At this present, communication is carried out using a protocol called TCP/IP, which was developed several decades ago for an entirely different reason. IP-based security protocols that are dependent on communication channels while the data itself needs to be secured already exhibit their limitations as deployment of Internet of Things (IoT) becomes more widespread. NDN is an architecture that falls within the most general category of ICN and has similar attributes and purposes on regards to the utilization of named data. To facilitate the effective dissemination of content and to emerge as a promising research for future internet architecture, since 2006, researchers in Europe and the United States have initiated several research projects concerning the architecture of the next generation of the Internet. These projects include DONA (Data-Oriented Network Architecture), which was proposed by the UC Berkeley RAD lab; 4WARD, which was funded by the European Union FP7; PSIRP (The Publish-Subscribe Internet Routing Paradigm); Content-Centric Networking (CCN) and Named Data Networking (NDN) is one of the five projects funded by the U.S. National Science Foundation under its Future Internet Architecture (FIA) program [12]. These initiatives, without exception utilize a content-centric approach to network architecture design. As a result, NDN has established itself as a representation and innovation station for next-generation Internet.

IP networks and CDN operate in a manner that is apparently close in terms of security. NDN provides a method that is both more secure and more effective in terms of data distribution. Data being sent through an NDN is provided a digital signature by the sender before it is transmitted. In IP networks, security has always been an afterthought, whereas in the NDN paradigm, security is built-in from the beginning. The retrieving process can be performed faster and with less overload. NDN make a transition from point-to-point packet delivery to named content. The objective of naming is not only to uniquely identify content objects in the network, but also to include important properties such as pertinence, usability, scalability, and security [13], [14]. In comparison to traditional networks, NDN's original design already have included security mechanism. Unlike IP networks, which strive to protect link connections, NDN focuses on content security. Despite the advantages of ICN features, it still has flaws that malicious users might exploit. To accomplish this, content integrity should be maintained, and attacks should be recognized and mitigated to their ability. In this study, we investigate the integrity and authenticity of content in the NDN, as well as the possibility of an attack on the integrity of the content and the existing mechanisms to address this issue. Despite these challenges, given the fact that NDN possesses a variety of built-in security features that still contain flaws that have not yet been resolved. After providing an overview of the NDN project, we will now present a concise examination of these security concerns, as well as pertinent attacks and the countermeasures that NDN implements to prevent them.

A. CONTRIBUTIONS

As a potential architecture for the future internet, NDN is anticipated to be resistant by design to both existing and new attacks. However, NDN is unfortunately susceptible to a variety of attacks that target its in-network caching technique like content poisoning attack [15], [16]. Motivated by previous literature, this review article focused on preserving data integrity in ICN. The main contributions of this survey can be summarized as follows:

- We analyze three types of attack that target to harm the data integrity in ICN. Attacks reviewed are

Man-in-The-Middle attack, replay attack, and Content Poisoning Attack.

- We overview each attacks and disscuss the countermeasures along with its limitations.
- We provide an open research issue for all three attacks, which will serve as a resource for new NDN researchers.

This review article examines security attacks in the NDN for which there are no better approaches currently available. The trust model is used to address privacy challenges such as the name, signature, and cache privacy will not be covered in this article. To the best of our knowledge, we are the first to publish a comprehensive survey on these three types of attacks against NDN. We address each one of these three attacks separately, reviewing the current state of the art and flaws of proposed mitigations and alternative techniques in the process. In addition, we discuss current challenges and future research direction for new path.

B. RELATED SURVEYS

NDN is a promising future design for the Internet, and as such, it has garnered a significant amount of attention from both academia and industry. Furthermore, in the past few years, it has emerged as a topic of intense interest in the field of network research. The NDN architecture may be vulnerable to a variety of different attacks, even though the network was designed to ensure data security using its built-in primitives (i.e., cryptographically signing data objects by the producer). On ICN, some good survey work has recently been performed. As a response, we have included this section to clarify the differences and relevance of each one. Survey on ICN in terms of mobility, naming, routing, and caching was performed in [17] and [9], exclusively on NDN can be found in [18]. Authors in [19] discussed in-depth research of various components of NDN that includes routing, forwarding, security, and mobility. However, with the security attacks that has been surveyed, the security goals that are compromised is ignored. Then, when we shift our attention to a specific domain, surveys that highlight the content security and attack threats in ICN and NDN can be found in [20], [21], [22], [23], and [24].

Authors in [20] discussed and classified attacks on ICN into four categories: naming, caching, routing and miscellaneous. Primarily, author main focuses on methods which an attack being performed in detailed and the solutions that are currently used in IP-based to be reused in ICN. The NDN community has come to an agreement on an attack like Content Poisoning Attack (CPA) and Interest Flooding Attack (IFA) are significant threats to NDN, IFA will be out of scope of this paper, and has been reviewed comprehensively in [25], [26], [27], [28], and [29].

The authors of [21] discussed security issues of ICN, which contrasted with the security aspects discussed in [20]. The authors categorize security aspects into three categories: security, privacy, and access control. Authors concentrated on mitigation strategies approaches and privacy considerations, although the surveys conducted were not specialized in the NDN element.

The authors of [22] concentrated on the privacy element of NDN and classified it into five categories: cache privacy, content privacy, name privacy, signature privacy, and trust management. Attacks on privacy have also been mentioned, such as denial of service (DoS) [30], timing attack [31], and protocol attack [32]. The technological component of countermeasure limitation, on the other hand, is not mentioned.

According to the authors in [23], they survey the security aspect of ICNs by highlighting weaknesses, threats, and solutions against them in a concise manner. There is a broad perspective on security threats in numerous ICN instances such as NDN/CCN, Network of Information (NetInf), and Publish-Subscribe Internet Technology (PURSUIT) in the surveys, but no specific attacks are mentioned in the countermeasures section.

Authors in [24] covered attacks in NDN, such as cache privacy attacks, cache pollution attacks, interest flooding attacks, and content poisoning attacks. Authors also addressed detection and mitigation strategies for each sort of attack; however, they did not outline future research directions for the reader.

In brief, the relevant surveys such as those from the entire area of ICN and NDN as well as the surveys from a particular domain in ICN, are described in depth. Based on the research presented above, the thorough sketch of the NDN security is lacking. To begin, the surveys conducted across the entirety of the ICN and NDN fields always provide a vague and general representation on security aspect. There has been a range of previous work on content integrity attacks, but our article focuses on three sorts of attacks that are specifically aimed at the integrity of the content.

II. INFORMATION CENTRIC NETWORKING

This section offers an overview of the fundamental components of ICN by elaborating on Named-Data Networking (NDN) and Content-Centric Networking (CCN), both of which are extensions of the overall ICN design. If the reader is already familiar with the topic and these potential interpretations, they will not miss any certainty by skipping this section.

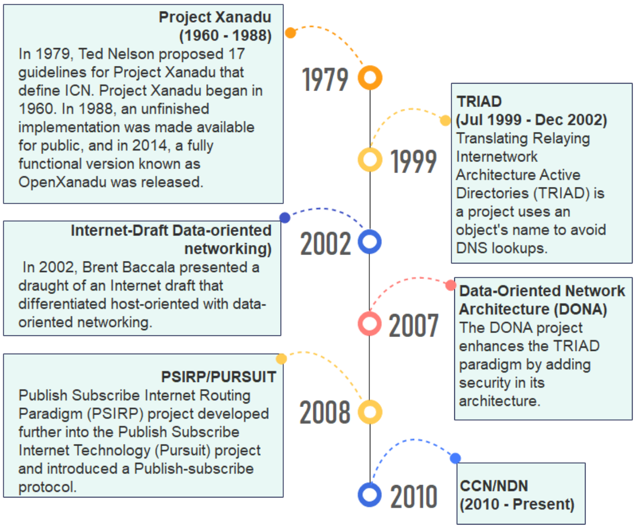
A. OVERVIEW OF INFORMATION-CENTRIC NETWORKING

Users access the Internet in order to receive various types of content, including web pages, audio content, and live video streaming. These people are primarily concerned with what they download and they have little interest in the locations where stuff is stored. Traffic growth has evolved and raise the bar by requiring a very-high bandwidth requirement under low latency constraint. On the Internet, source and destination are both identified by their respective numeric IP addresses and is almost exclusively employed for the distribution of content on a large scale. The misunderstanding that exists between how people use the Internet and the services that are provided by IP networks is at the root of several issues, including those pertaining to usability, performance, security, and mobility. As a result of this paradigm shift, the focus is shifting away from IP and toward blocks of named content.

Where ICN enables consumer to request the content they want using application layer names also enable NDN to secure data directly at the network layer.

The question of whether the Internet requires a new clean-slate design or whether we can continue "patching over patches" has been brought up in the work [33] and ICN's configuration is one of the major aftereffects of the many different global future internet research initiatives that have taken place. In 1979, Ted Nelson's idea, which he called the "Project Xanadu", included a set of 17 recommended regulations. The ICN can be developed in response to these 17 guidelines, which serve as its guiding principles. The beginning of Project Xanadu may be traced back to 1960. However, it took a very long time to bring Project Xanadu to the public's attention. Then, the idea of an ICN was first put into practice in the project called Translating Relaying Inter-network Architecture integrating Active Directories (TRIAD) [34] in the year 1999. TRIAD is the first that treats content as first-class while changing the communication from the host-centric to content-centric communication. The approach reveals the shortcomings of the existing models for the distribution of content, whether those shortcomings are related to latency, scalability, architectural openness, and consistency. TRIAD handles the content problem by explicitly defining a content layer that is capable of routing towards content in an efficient manner. The content layer extends the capabilities of typical IP routers to provide name-based routing, thereby spanning the entirety of the network's core. After that, In the year 2007, UC Berkeley and International Computer Science Institute (ICSI) collaborated on a new project that was given the name Data-Oriented Network Architecture (DONA) [35]. The DONA project makes TRIAD better by elevating security (authenticity) and persistence to the level of first-class primitives within the architecture. The "Future Internet Architecture" (FIA) [36] program was initially introduced by the National Science Foundation (NSF) in the year 2010. At its beginning, the (FIA) was a 5-year initiative with the objective of establishing a set of candidate architectures for the future generation of the Internet.

In 2015, the NSF reaffirmed its dedication by launching a follow-up program titled "Future Internet Architecture – Next Phase" (FIA-NP) [37]. In contrast to FIA, which was primarily concerned with architectural research, FIA-NP focusses on evaluation that is accomplished using prototypes, testbeds, trial deployments, and intensive experimentation. Several research initiatives that showed NDN milestones can be seen in Fig. 1, including those supported by the United States funded projects are: Data Oriented Network Architecture (DONA) [35], MobilityFirst [38], Content-Centric Networking (CCN), Named-Data Networking (NDN). While in European funded projects: Publish-Subscribe Internet Routing Paradigm (PSIRP)/ Publish-Subscribe Internet Technology (PURSUIT) [39], [40], [41], 4WARD [42], CONVERGENCE [43], Scalable & Adaptive Internet soLutions (SAIL) [44], and COntent Mediator architecture for content-aware nETworks (COMET) [45].



Project Xanadu (1960 - 1988)
In 1979, Ted Nelson proposed 17 guidelines for Project Xanadu that define ICN. Project Xanadu began in 1960. In 1988, an unfinished implementation was made available for public, and in 2014, a fully functional version known as OpenXanadu was released.

TRIAD (Jul 1999 - Dec 2002)
Translating Relaying Internetwork Architecture Active Directories (TRIAD) is a project uses an object's name to avoid DNS lookups.

Internet-Draft Data-oriented networking)
In 2002, Brent Baccala presented a draught of an Internet draft that differentiated host-oriented with data-oriented networking.

Data-Oriented Network Architecture (DONA)
The DONA project enhances the TRIAD paradigm by adding security in its architecture.

PSIRP/PURSUIT
Publish Subscribe Internet Routing Paradigm (PSIRP) project developed further into the Publish Subscribe Internet Technology (Pursuit) project and introduced a Publish-subscribe protocol.

CCN/NDN (2010 - Present)

FIGURE 1. Timeline of NDN project.

Even though these projects take unique approaches to their own designs, they have several architectural characteristics, goals, and presumptions in common with one another. The CCN/NDN, which is one of these efforts, is gaining more importance due to its clean and feasible architecture. Namely by exchanging the IP architecture for the one that uses named contents.

B. NAMED DATA NETWORKING

Van Jacobson introduced NDN for the first time in 2009. It swiftly received positive feedbacks from a community of researchers, and National Science Foundation's Future Internet Architecture (NSF-FIA) projects support and has since become a focal point in the quest for next generation of Internet architecture. NDN architecture one of the NSF projects and is a detailed implementation of CCN [7], unlike IP architecture where it revolves around end-points and delivers packets to hosts based on numeric IP addresses, NDN revolves around named-content that is composed of one or more variable-length components that is addressable and routable at network layer.

The traditional architecture of the Internet was first and foremost intended for the communication purpose between essentially two devices. Most data transferred across the Internet is comprised of connection-oriented TCP conversions carried out by pairs of hosts communicating with one another. On the other hand, even though the Internet has been expanding at a significant rate, the scope as well as its uses have undergone significant adjustments. The era of "Big Data" has begun, and concurrently, the primary application mode has shifted from text communication to information accessing and distribution. End-to-end communications that are designed for current internet architecture will embrace a challenge facing this transition. There are several issues that arise in terms of the security, mobility, and efficiency. Because of it, the NDN architecture has been developed to these issues.

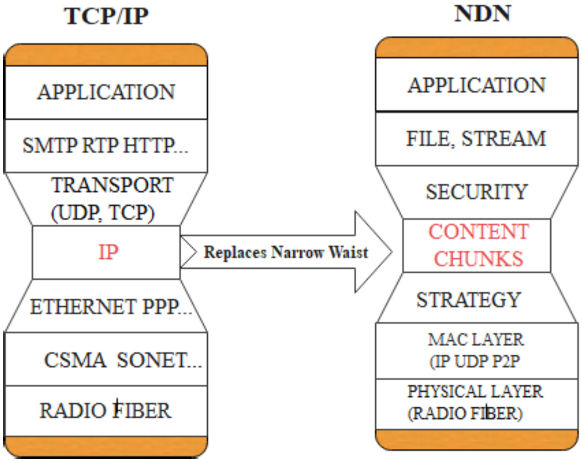


FIGURE 2. TCP/IP and NDN hourglass stack.

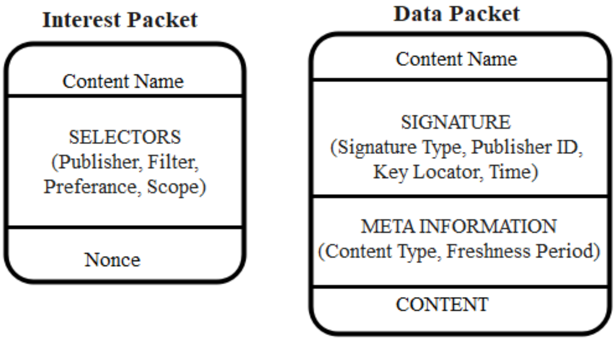

Interest Packet
Content Name
SELECTORS (Publisher, Filter, Preferance, Scope)
Nonce
Data Packet
Content Name
SIGNATURE (Signature Type, Publisher ID, Key Locator, Time)
META INFORMATION (Content Type, Freshness Period)
CONTENT

FIGURE 3. NDN packets.

The hourglass form of the IP architecture is inherited by NDN, but the receiver-driven data retrieval model takes the place of the end-to-end data delivery model at the narrow waist of the hourglass as shown in Fig. 2, where it shows the hourglass architecture of both NDN - (right side) and TCP/IP - (left side). With this fundamental shift, the emphasis of the Internet architecture from its current "where" (location) to "what" (content), with the primary focus being placed on named content (Data) rather than IP.

TCP/IP involves the combination of both the source and the destination addresses to establish a point-to-point path. The path that connects the two endpoints is the route that packets take when being sent between them. However, with the NDN architecture, any intermediary node that possesses a copy of the content that is being requested can respond. While NDN is an innovation, it does represent an important advancement over IP in a way it represents a paradigm shift from host-based to content-based oriented communication. In which, communication revolves around users by changing the transport layer in the network protocol stack, i.e., NDN utilized a pull-based communication model in which content was delivered upon user request. Interaction between nodes is accomplished by the exchange of interest and data packets. Where as shown in Fig. 3:

- **Interest packets**: Stores information of Interest packets that has not been resolved with a given response. Network congestion prevention is the task PIT holds if router receive more than one request for the same content.
- **Data packet**: Same as the one in TCP/IP architecture. Store content names and the corresponding routes for interest packet.

The headers of NDN packets do not have a predetermined length. It contributes to the reduction of the cost of processing packets. Therefore, smaller packets can be transported without the need for additional overhead. It provides the packets with greater adaptability. In instead of headers with a predetermined length, the design makes use of the Type Length Value (TLV) format, which allows for the easy modification for new types. This feature is equipped to handle the potential that in the not-too-distant future that the protocol may undergo further development, which could result in previous type being obsolete. This is an additional benefit in comparison to TCP/IP. Data packets and interest packets can be differentiated from one another based on the type field.

The Content Name and the Nonce are the two key components that made up an Interest packet. The desired data's name has been specified using the content name. The combination of the name and the nonce fields provide a distinctive identifier for interest packets. The consumer is responsible for the random generation of the nonce and it serves the purpose of differentiating between two distinct users who have requested the identical piece of content. It's plausible that a user may send their interest multiple times and it is also possible to identify this with the assistance of Nonce. Thus, when router receives an identical interest packet from the same consumer then will be forward on different interfaces.

NDN employs a hierarchical naming scheme [46] that is human readable and this naming scheme is applied for forwarding, routing, and retrieving the content on the network. The hierarchical naming method is similar with the Universal Resource Identifier (URI) [47] and the naming conventions used by application developers can be configured to suit their specific goals and objectives. In the typical encoding URIs, component boundaries are indicated by the character "/," which serves as an explicit delimiter. As an idea, the name for news article from CNN and was published on January 1, 2016, would look something like this: /CNN/news/10jan2016. It is necessary to break up large sections of content into smaller bits or parts. For instance, the 643rd chunk of a film that Alice uploaded to YouTube and titled "sports.avi" could be referred to as "/youtube/alice/sports.avi/643."

The Interest packet is generated by the content requesting node and holds the desired content name as well as content-related security information. To maintain the content integrity, any node in the network that has the matching content responses with the data packet along with its native security mechanisms, such as digital signatures. The name identifies the content itself, and not the producer, publisher, or forwarder of the content, nor the location where they are located. Now with this feature, the network is protected from some directed denial-of-service (DoS) attacks. In the meantime, routing and forwarding in NDN is supported by three different data structures:

- **Pending Interest Table (PIT)**: Stores information of Interest packets that has not been resolved with a given response. Network congestion prevention is the task PIT holds if router receive more than one request for the same content.
- **Forwarding Information Base (FIB)**: Same as the one in TCP/IP architecture. Store content names and the corresponding routes for interest packet.
- **Content Store (CS)**: The CS caches Data packets of satisfied Interest request and be used for future Interest request.

The CS keeps a copy of the data packet that was sent in case if it is needed later. The CS keeps a copy of the data packet that was sent in case if it is needed later. The PIT oversees monitoring pending Interests, whereas the FIB is a lookup table that is used to forward an incoming Interest packet to the appropriate destination. The first thing that NDN node does when it receives an Interest packet is to search the CS for a data packet matches the Interest. Assuming it exists, it means that the packet originated at CS and was transmitted straight to the same interface from which the Interest was received. When there is no perfect match for a PIT entry, it just adds the Interest's arrival interface in its entry inside the Interest's PIT. If there is no compatible PIT entry, the router searches for the longest prefix match [48] in the FIB; the Forwarding Strategy then selects the output interface(s) in accordance with this match in the FIB. The data packet is returned to the consumer after being routed through the PIT entries in the right sequence.

C. NDN SECURITY

In comparison to traditional TCP/IP architecture, NDN design provides data integrity and authenticity using digital signatures. At the time of content production, a producer can make use of the NDN to generate a digital signature that will be assigned to each data packet. Not only that, but the access control capabilities also that are adopted helps in ensuring the only legitimate users can access the content that is specifically tailored for each of them [21].

Security aspect that are implemented in NDN is based on data-centric security model techniques that are not related to either the content location or the host, and in which the data packets are signed by the producers. Thus, content integrity and authenticity are preserved and any content indirectly enforced to have public key signatures [49]. NDN has offered fundamental approaches for ensuring content integrity and authenticity, as well as for ensuring the authenticity of content. To be more specific, content must be digitally signed by its publisher's private key so that the integrity of the content can be validated afterward by its consumers or network routers, whenever they receive data from either the publisher or other routers that use the publisher's public key to sign the messages. A signature ties content to its content name and ensures that the content's integrity, validity, and correctness are maintained regardless of where and when content is retrieved. NDN may not require the establishment of a specific certification infrastructure, instead opting for the outsourcing of trust management to compatible services [50].

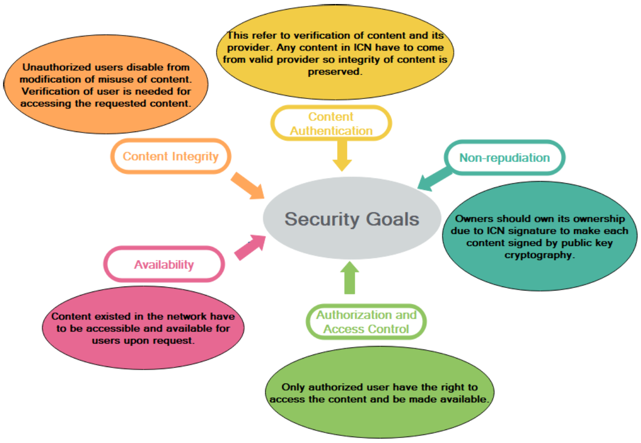

This refer to verification of content and its provider. Any content in ICN have to come from valid provider so integrity of content is preserved.
Unauthorized users disable from modification of misuse of content. Verification of user is needed for accessing the requested content.
Content Authentication
Content Integrity
Non-repudiation
Security Goals
Owners should own its ownership due to ICN signature to make each content signed by public key cryptography.
Availability
Content existed in the network have to be accessible and available for users upon request.
Authorization and Access Control
Only authorized user have the right to access the content and be made available.

FIGURE 4. Security goals.

In addition, security adheres to a data-centric model, highlighting the necessity of ensuring content integrity and source authentication. In the case of a content-centric based architecture where the contents can be found and delivered at any point in the network and not only by the original material creator, but also by the features are especially important. ICN is working hard to attain this goal. The producer always signs the contents, allowing consumers should always verify content integrity and data origin. Security goals is shown in Fig. 4 [37].

In the face of many great benefits in implementing ICN paradigm, the fundamental transformation represented in the network layer inevitably comes with a new security concerns. For an example, every ICN implementations must have a name-content integrity verification technique that allows users to determine whether the retrieved content has been tampered with. Furthermore, content authenticity should be addressed to provide a method in determining content origin.

In ICN, securing the content is far more critical than securing the infrastructure or end points. When approaching the final ICN paradigm, the lack of addressing security goals is even more significant. As shown in Table 1, each of the attack correspond to the security goals parameter that are affected. Certain standards must be met to provide security services. To take advantage of ICN's fundamental security feature of preserving content integrity, the name should establish a connection between the name and the publisher's public key (in verifying the signature). Following that, to ensure the authenticity of the data, the name should establish a binding relationship with the content via a digital signature.

As integrations of ICN to IoT is widely used in providing a security aspect, there are several applications use-case that utilize ICN in their deployment [51], [52], [53], [54], [55], [56], [57]. As one of the applications where security is important is in healthcare field. Authors in [58] proposed body sensor network (BSN-Care) that is used for IoT-based healthcare system. Authors addressed security goals like authentication, anonymity, secure localization, content privacy, and integrity by proposing a two-party authentication protocol named lightweight anonymous authentication protocol (LAAP). In the BSN-Care system, LAAP protocol is responsible in ensuring the security goals like authentication, anonymity, and secure localization properties. Proposed system consists of two phases: registration and anonymous authentication phase. Where in registration phase, the BSN-Care server issues security credential to local processing unit (LPU) in ensuring the identity. While, in anonymous authentication phase, both LPU and server will authenticate each other. Even without the context of ICN in their deployment, utilizing AES encryption may cause burden to router if integrate with ICN. While authors in [59] proposed mobile Named Data Network of Things for Healthcare Services (NDNoT) that us efficient using named content in peer-to-peer model. Utilizing the encryption-based access control to secure the user.

With security that NDN provides, there are attacks that occurred in NDN that will affecting content integrity like replay attack, man-in-the-middle-attack (MITM), and content poisoning attack.

III. MAN-IN-THE-MIDDLE ATTACK (MiTM)

The data-centric retrieval approach of NDN permits explicitly securing the data itself, as compared to securing the channel between the sender and the receiver as is accomplished in traditional IP networks. In particular, data-centric security in NDN needs to accomplish three primary goals: 1) Data Integrity, which states that the data cannot be altered once it has been produced; 2) Data Authenticity, which states that the data is produced by the claimed producer; and 3) Access Control, which states that only consumers (producers) with required permissions can access (publish) the data. The NDN has made direct use of public key cryptography in order to accomplish these objectives. One of the integrity attacks is the Man-in-The-Middle (MiTM) attack [60], this attack is performed by using third parties or malicious node to intercepts and gain control of the communication channel between two nodes, usually the nodes is end-user and router. MiTM existed quite some time and it as not as common as other types of attack as DoS in NDN architecture. MiTM main abilities is to secretly gain control by intercepting packet that passes on the communication channel. In NDN network, MiTM can wrapping two or more data packet with the same name but different in content and signing it with its own key as shown in Fig. 5.

The objectives of MITM are to compromise the integrity of the content, and this can be accomplished at various layers of the Open Systems Interconnection (OSI) model. MiTM attacks can be classified into two categories, namely:

- **Passive MiTM**: In passive MiTM, attacker focusing on monitoring the traffic between the user and end user. Passive MiTM does not involve altering the packet but have the goals to know the content that being shared.
- **Active MiTM**: In active MiTM, attacker will monitor, captures and records traffic between victims. Content integrity is not preserved due to breach of content. Active MiTM brings severe damages to victim.

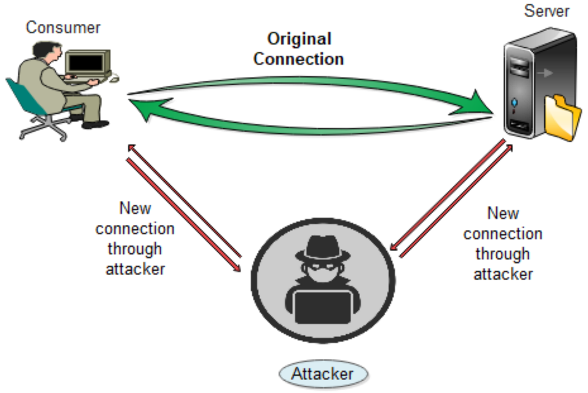

Consumer
Original Connection
Server
New connection through attacker
New connection through attacker
Attacker

FIGURE 5. MiTM attack.

A. MITIGATIONS TECHNIQUES

Countermeasures against MiTM include the use of a credible digital signature to ensure the integrity and authenticity of the packet by binding the name of the content to the packet.

1) NAME-BASED ACCESS CONTROL

Due to one of the NDN features is in-network caching. Encryption-based access control is one of the methods selected to verify the content integrity and authenticity. In [61], authors leverage identity-based encryption, identity-based proxy re-encryption and decentralized identifiers to provide support for content integrity by proposing name-based security for ICN (NBS-ICN). The integrity is preserved by digital signature generated by the owner at the same time content authenticity can be verified. Simple challenge-response protocol used for user authentication where registry generates random number for user to respond with digital signature of that number, every exchanged message taken place over TLS thus will prevent MiTM attacks. The drawbacks are management of secret key distribution that is generated by the producer. Access Control is an essential component of the modern Internet since it decides which users are permitted to access the content in and should be taken into consideration in designing a secured system.

2) IDENTITY-BASED ACCESS CONTROL

Authors in [62], design attribute-based access control mechanism for Publish Subscriber Internet-ICN (PSI-ICN). A generic rendezvous point is employed in this technique, which performs an entire information query and these network nodes mediate content demand and supply to handle access control regulations. Additionally, this approach proposes an identity-based proxy re-encryption to protect content from the content provider. Because of their access control measures, the content will be encrypted independently. Two identifiers, the rendezvous identifier (RId) and scope identifier, will be used to identify the content (SId). SIds are one-of-a-kind globally, while RIds are one-of-a-kind

TABLE 1. Security Goals and Integrity Attacks in NDN.

Categories	Attack	Targeted layers	Authentication	Availability	Integrity	Confidentiality
Content attacks	Man-in-The-Middle	Network Layer	Yes	Yes	Yes	Yes
Routing attacks	Replay attack		Yes	Yes	Yes	
Cache attacks	Cache pollution attack	Application layer		Yes		
	Content poisoning attack			Yes	Yes	

inside a scope. SIds are used to provide a "clue" regarding a content item's network location. A lookup node called as the rendezvous node manages each Sid in particular (RN). Where the 'RN' maintains a 'SId' as the SId's rendezvous point (RV). The 'RV' of a 'SId' keeps track of a data structure that maps the SId's RIds to publisher network locations. The rendezvous network is a network that connects all the RNs.

3) SIGNATURE-BASED ACCESS CONTROL

Lightweight mechanism for integrity verification and access control (LIVE) was proposed in [63] and was an extension of NDN. The existing signature verification is heavyweight and lead to content corruption. Live generates one-time signature token with lightweight access control scheme for content so that only legitimate users have its own private tokens that can be used to access the content thus preserving the integrity. Process of LIVE verification is 20 times faster compared to traditional public key, but the one-time key signature concept will face a challenge of distributing the token. One-time signature (OTS) algorithm concept later used in authors further work [64] as capability-based security enforcement architecture (CSEA), the main difference between both is access control policies in LIVE is enforced in centralized manner; whilst the latter allowing distributed access control which token generated by content producer that have disadvantages to lose ability in in-network cache. Other lightweight verification and authentication is [65] and [66].

4) NAME-SIGNATURE LOOKUP SYSTEM

Verifying packets using Name Signature Lookup (NSLS) and name lookup protocol (NLSP) proposed in [67] to eliminate MITM attack. Authors proposed name signature lookup system (NSLS) and corresponding name-signature lookup protocol (NSLP) to be used in verifying packets with registered publisher even the communication take place in untrusted network, with the help of Network Interface Controller (NIC) within keys inside. Two algorithms produced namely and digest/hash algorithm where the latter used to make message digest for indicate message integrity. While signature algorithm uses private key from pair of asymmetric to sign the high value of message. MiTM attacks are eliminated by make sure NSLP protocol performed accordingly.

IV. REPLAY ATTACK

In the replay attack [68] that is also known as playback attack, is shown in Fig. 6. Attackers act as unauthorized users to intercept the transmission of data and save a copy of messages that will compromise the content integrity of the messages, messages are saved and will be resent later to cause harm. The replay attack is one of the man-in-the-middle attack variants, and most replay attacks are passive in their behavior. When it comes to maintaining data integrity and authenticity in NDN, a replay attack can be a significant obstacle. The following measures can be taken to avoid a replay attack:

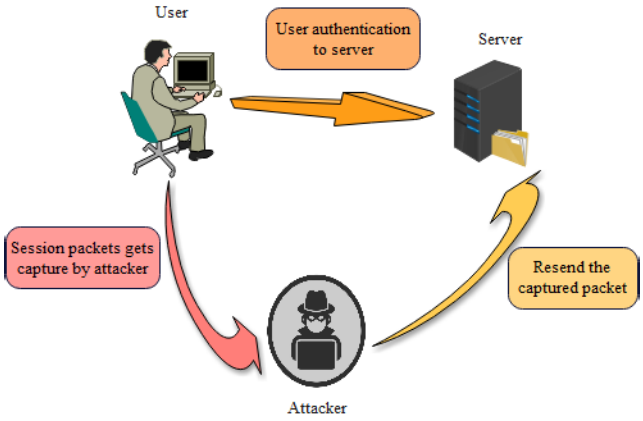

User
User authentication to server
Server
Session packets gets capture by attacker
Resend the captured packet
Attacker

FIGURE 6. Replay attack.

- **Digital Signature:** A timestamp and nonce are used to generate signatures on data packet that includes a unique identifier, allowing the requester to prevent any repeated timestamps during the data request process [69].
- **Session Key:** CS stores Data packets from satisfied Interest requests in a cache, which can then be used for future Interest requests. Session keys that are time-specific, cannot be recycled which is used as a one-time permission for requesting that helps in preventing an attacker from resending falsely recorded packets once they have been captured [70].
- **Integrating Blockchain Technology:** In order to maintain the integrity and validity of the content in NDN, certain technological integrations can be utilized. Recent developments have seen the integration of NDN and blockchain technologies in the realms of security and IoT in the provision of security [71], [72], [73], [74], [75]. Bitcoin and blockchain technology have the capacity to manage efficient data retrieval while also providing data security. When blockchain is used in a typical IP network, compatibility concerns exist; however, when blockchain is deployed in NDN, a different outcome can be accomplished, resulting in improved performance.

The replay attack, which is frequently used to circumvent authentication systems and the preventive mechanism described above, must be built effectively in terms of preventing computational overhead. As for now, content is cached on certain specified servers, which assists to speed the process of downloading web pages. This makes it much easier for network security administrators to configure the various security modules on the network in today's Internet infrastructures. As a side benefit, the processes for access control become more comprehensible. This ability to retrieve content from multiple different locations at the same time is made possible by the inherent property of in-network caching. As a result of this feature, the access control security service in ICN is far more complex than it was in the past. Furthermore, the access control component ensures that the ICN's confidentiality and integrity are preserved.

There are three ways to mitigate replay attack in NDN: timestamp and nonces [76], [77], [78], [79], authentication [70], [80], [81], [82], [83], [84], and the use of blockchain [85], [86].

1) TIMESTAMP

By including a timestamp and nonce in the Interest packet signature, it is possible to effectively defend against this type of attack. Upon receiving an incoming request Interest, the signer can compare the timing of the request to a predetermined time frame. Aside from that, the signer can preserve a short state, such as a bloom filter of the nonce values that have been observed from recent queries. As a result, the attacker was unable to replay because there will be no interest packet whose timestamp is before the present time by the timeframe and who's nonce is not being viewed by the signer. In ICN, developers should address the access control restrictions for distributed cached material. The authors in [76], suggest an Attribute-Based Encryption [87] naming scheme to deal with the distributed management of content characteristics via an ontology-based management system and the enforcement of access regulations on public or cache-able routers via a set of name attributes. As the proposed mechanism, which makes use of a trusted third party (TTP) in the network, can preserve content privacy and prevent replay attacks. With the presented scheme that employs flat naming and makes use of TTP, it has several limitations, the most significant of which is that it cannot be used to hierarchical naming systems and that deployment in the IoT may not be possible due to the presence of TTP in the network.

In a study done in [77], authors proposed Interest-Based Access Control (IBAC), which is access control technique that uses information in interest packets to impose access rules. The proposed approach will make unpredictable content names to unauthorized user. Name obfuscation is supported using either hash- or encryption-based techniques. Access control rules and content encryption are decoupled in this method, allowing the original content producer to apply any access control rules without having to deal with content encryption or key distribution. A mutual trust verification structure is created between producers and consumers to enable routers to conduct authorization checks before forwarding interests to local caches and prevent interest replay attacks.

Authors in [78], built an anonymization method for content-centric networks to avoid censorship. Author created a Consumer-Driven Access Control (CDAC) method that includes encryption-based access control in interest names and allows the producer to recycle specified material stored at intermediate content stores along the communication path. In the initial phase of communication, plain-text routable names are used, while encrypted names are employed to offer anonymity. Mitigations of replay attack inspired by [78] and censorship by [88], the main difference it held is the previous paper focused on encrypting the names in deterministic manner while get rid of in-network caching feature, while [78] proposed consumer-driven access control of network nodes that can make use of in-network caching. The proposed system's fundamental flaw is that it primarily targets on-path intermediate nodes, leaving stored stuff off the communication path unrecyclable [89].

Authors in [79] proposed decentralized access control protocol for ICN (DACPI) that required fewer public messages in deployment of access control in between ICN subscribers and ICN nodes that utilize self-certifying naming scheme. Security analysis include man-in-the-middle, replay attack and user privacy. DACPI made use of RSA public key infrastructure, exchanging of keys by Diffie-Hellman (DH) enabling content dissemination to have decentralize access control. Cached content stored is in the form of plaintext that prone to content poisoning attack.

Authors in [90] proposed a privacy preserving E-health solution in NDN to ensures privacy and integrity aspect of the content security. Authors adapt Andana [91] on top of Identity-based cryptography (IBC) primitives to create a valid public key. Authors further their work in [92] that improves their earlier solution that focusing on performance aspect. Authors demonstrate the solution in IoT environment to prove in terms of security attacks, by utilizing naming scheme then generates three symmetric keys used to wrap the interest name and encrypt the data packet it able to mitigate attack like eavesdropping attack, replay attack, known key security and time correlation attack. Overhead evaluation comparison shown IP still lowest in terms of integrating Andana to its mechanism and this cannot be a result currently due to optimization and limitation in NDN software haven't been fully advanced for simulation purposes.

From past research, with NDN, using and choosing the right cryptographic scheme can prevent from malicious attack and harm to a content. Another cyber-physical system in e-health [93] using NDN-based certificateless signcryption using hyperelliptic curve cryptosystem (HCC). Authors consider creating a mechanism that is appropriate in terms of minimizing computing and storage overhead, with this, by utilizing HCC that have low complexities, less storage and smaller key size is suited best. Security aspects taken include confidentiality, authentication, integrity, and replay attack.

Multiparty signing in NDN (NDN-MPS) proposed in [94] to support multiparty signature signing and verification for resource control in smart grid. The design of the NDN, as well as its implementation in the NFD. The NFD

(NDN Forwarding Demon) [95] is the reference implementation of the network forwarder for the NDN protocol. It is a free and open-source software that improves in conjunction with developments in NDN research. As mentioned by the author, The interest packets can also be used to create a signature, which is referred to as the signed interest. It is an optional way to establish an authenticated the sender, supporting the receivers' ability to authenticate the command; however, it is recommended. A date and a nonce are also included in the signed interest to prevent replay attacks (with novel timestamp and nonce). When a user gets a signed interest, user may be able to validate the signed interest by using the trust model, which is like the data packet validation model.

2) AUTHENTICATION

Insight gained from past study showed that digital signature can be used to certify the message's integrity. Producer can select type of signature algorithm used like RSA, DSA, ECC, EC-DSA. Ensuring content integrity and authenticity requiring content signature native features in NDN. Using variety of digital signature scheme has been proposed in [96] to preserve content integrity and achieving authentication. Not only that it also includes post quantum signatures, network coding signatures and privacy preserving signatures. Authors performed an operation to speeding up signature generation and verification. Not only that, but authors also aim to reduce the signature bandwidth where the communication cost is a major issue of signature performance since signature transmission usually consumes more power than that of signature generation and verification. ICN is subjected to security threats from an attacker who could be a producer, a client, or a man-in-the-middle attacker. These attackers can perform an active attack in the manner of impersonation, alteration, replay attack, or a passive attack in the form of eavesdropping, or they can launch both active and passive attacks simultaneously. Digital signature-based access control mechanism in Information-centric Network (DSAC) is proposed in [49], with the goals to enhance security in ICN. Proposed mechanism utilized digital signature, trusted third party (TTP), proxy TTP and hash function and has shown an improvement in integrity, authentication, and confidentiality.

Lightweight cryptosystem that incorporated elliptic curve cryptography for CCN (CCN-ECC) to ensured security proposed in [80], then authors further work into secured content dissemination for CCN using elliptic curve cryptography based public key infrastructure (ECC-PKI) [70]. The proposed scheme aims to minimize computation overhead while increasing the security, performance, and efficiency. Formal verification testing is implemented to concludes the scheme that it is secure against attacks.

3) BLOCKCHAIN

There have been numerous attempts to determine the applicability of blockchain technology for ICN in a variety of different disciplines over the years [97]. NDN and Blockchain recently have been integrate in domains of security and IoT as it can manage efficient data retrieval and guarantees data security [71]. Hierarchical identity-based security mechanism using blockchain (HISM-B) in NDN proposed by [98], utilize security extension on hierarchical identity-based cryptography (HIBC) algorithm to generate elements that is needed for authentication in NDN. The HISM-B uses two authentication validation that is on producer signature for data packet and domain signature for producer authentication. HISM-B more secured than NDN testbed provided that utilize one authentication that is for the data packet itself, main issues that arises is the time taken for signature generation and signature verification process. The questions of "does performance aspect matter in providing security in content integrity and authenticity needs to be considered?".

Authors in [86] proposed framework called BlockAuth that is based on blockchain to provide an efficient and lightweight solution for successfully authenticating mobile producers in a distributed manner. In their paper, the authors say that BlockAuth is a unique architecture that, using blockchain technology allows mobile device users with safe, fast, and reliable authentication for mobility management situations on the Internet of Things. In addition to authenticating product prefixes, it forces them to only express the original routing updates of the prefixes that they are permitted to publish. The authors have proved the efficiency and viability of their method by comparing it to criteria such as router throughput, authentication delay of the producer, and storage expenses. Furthermore, the framework is able of dealing with a variety of networking attacks, such as Prefix Hijacking Attacks, Denial of Service Attacks, Appending Attacks, Distributed Denial of Service Attacks, Replay Attacks, Packet Discarding Attacks, and False Reputation, all of which are particularly dangerous for blockchain and mobile networks.

As attack like interest flooding, cache poisoning, data fishing, and replay attack cannot be avoided by conventional security solutions that utilize decentralized and dynamic content create an environment where it unable to prevent this from happening. Authors in [85] proposed a blockchain based for NDN-IoT. Author presents six-layer of conceptual model: physical, data, network, blockchain, contract, and application layer. The blockchain may be used to detect packet level attacks such as sniffing and replay attack because all packet transitions are recorded in the blockchain. This allows the blockchain to be used to watch either attacker has modifying packet content or replaying the packets. Even though hosts can circumvent access control rules, the transitions of packets provide a sign that illegal access has occurred. This is particularly true in the case of access control.

Authors in [99] and [100] suggest that in replay attack, the attacker performs a MiTM attack and attempts to obtain a copy of the message from the sender, following which he or she modifies the message and sends it to the recipient. The recipient believes that the communication has been forwarded to him by the original sender, whereas in fact it has been modified by an attacker with harmful intent and forwarded to him. A similar attack is not viable with NDN since the interest packet is recognized by its name and a nonce is used to ensure that the namespace is unique across all nodes in the network. When the same interest packet (with the same name and nonce) arrives at the router, the router considers the packet is a duplicate and replays it; as a result, the packet is purged from the PIT table. Thus, the NDN protects itself from the replay attack by enforcing network layer security policies by default. The communication model used by CCN is entirely focused on content. Content-centric networking (CCN) addresses material rather than location, allowing users to place their trust in the content and its original creator rather than the origin (which could be an arbitrary, potentially untrustworthy cache). The fact that TCP/IP requires direct interactions with a (trusted) content source makes keeping current content on much easier in ICN. On the other hand, it requires that outdated content not be replayed and a secure method of obtaining indication that a piece of content is the most updated version provided by its author [101].

V. CONTENT POISONING ATTACK (CPA)

NDN employs an in-network caching mechanism, in which a router can temporarily store any passing data objects and then use those objects to fulfill future requests. However, from our previous experience with the Internet, it indicate that a networked cache system like this one is susceptible to one of the cache-based attacks as shown in Table 1. During a content poisoning attack, the adversary uses as many hosts that have been infected (zombies) in order to poison the network by inserting bogus objects into the routers cache. In-network caching can bring benefits to user when being implemented in mobile ICN and some research focused on enhancing network flexibility and mobility management [102]. In this context, an attacker's purposes while launching a content poisoning attack is to overwhelm router caches with invalid content [103].

In CPA, interest packet will remain unchanged but data packet may be poisoned and this attack can be performed by (1) Compromised routers or (2) Collaboration between untrustworthy provider and consumer. There are two types of poisoned content in CPA [15]: corrupted and fake content. In both cases, the content being altered and integrity of content is jeopardized. In the first case, where content considered corrupted is when untrustworthy provider lacks the necessary signature information to sign the has been altered content thus process of verifying signature will fail and able to be detected. While, in poisoned content is where the untrustworthy provider has the necessary information to sign the packet, thus process of signature succeeds, even it is more difficult to performed, it can make the attack impossible to be detected.

Using forged signatures but legitimate names, an adversary injects fake content into the caches of CCN router(s) through compromised router(s) or storage area of attacker-controlled content source(s) with the goal of delivering malicious content to consumers on demand. To cause a denial of service (DoS) effect on the network, an attacker can gain control of some of the network's routers and collaborate with compromised content source(s) to manipulate the content as well as the signatures of malicious content chunks. As consumers repeatedly send requests for valid content, the network's routers are overloaded with PIT requests and their CPUs are exhausted.

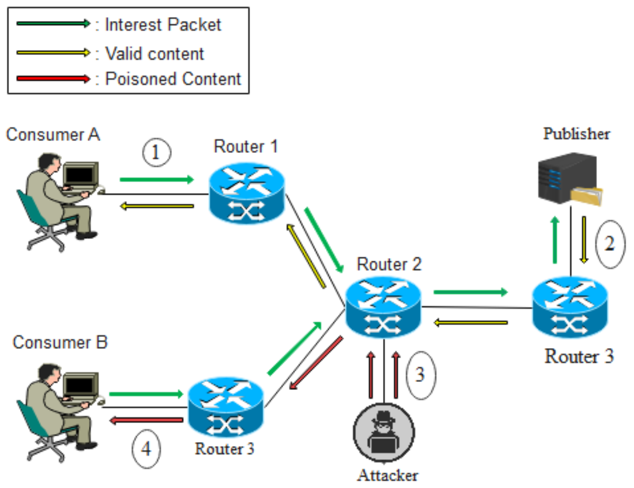


FIGURE 7. **Content poisoning attack.**

In-network caching features provide benefits to NDN architecture but they also have its drawbacks, such as the need to protect it from poisoned content, which pollutes the in-network caches of intermediate NDN routers and prevents consumers from receiving the legitimate copy of the content. The routes can be depicted in Fig. 7, started with (1): consumer A send an interest of desired content to router 1 notify publisher in providing the signed content. Default routing policy in NDN is open short-path first for named-data (OSPFN) [104], that is every intermediate node in between path able to store copy of the content. In (2), publisher will provide legitimate content with the legitimate digital signature across router 3, 2 and 1, and store the copies in content store. In (3), attacker send a corrupt response by injecting malicious content with fake signature to router 2. The poisoned content from the CS will get flows to router 2 and 3 and contaminates the intermediate router, thus consumer b receives the poisonous copy from router instead the legitimate content in (4).

An attacker must get control of one or more intermediate routers to be able to inject its own content into a network for this attack to become effective. However, the injected material has a fraudulent payload or a signature that is invalid, even though the material has a genuine name that corresponds to an interest. All ICN architectures are vulnerable to this attack, apart from those that are using self-certifying names [35] for host and content where names composed of cryptographically constructed and hash-verified in mitigating CPA attack. Having a secure routing could be the first line of defense against these kinds of assaults. If this is not taken into mind, however, the benefits of in-network caching in NDN may be severely limited if this is not performed with care.

There are two mitigations technique for content poisoning in NDN: signature verification and consumer dependent mitigation.

A. COLLABORATIVE SIGNATURE VERIFICATION

Many different potential preventative measures have been proposed. To begin with, authors in [15] consider among the first to addressed the issue of content poisoning attack in NDN. Authors proposed a countermeasure against attack such as cache poisoning and blackhole prefix hijack by establishing a strong bind between interest and the content by the utilization of self-certifying naming [114]. Authors proposed Self-Certifying Interest/Content (SCIC) that allows router to operate securely and able to return the legitimate content for interest requested. SCIC gets divided into two variants: the first is for static content (S-SCIC) and the other one is for dynamic content (D-SCIC). Combination of both variants offers a flexible approach in mitigating content poisoning attack. The drawback of proposed mechanism is that it adds extra burden to the router and that will lead to not an option for a cost-effective procedure.

In [115], author presented a lightweight content poisoning attack mitigation technique that aims to achieve low processing time and storage overhead. The proposed scheme makes the publisher divides a data packet into two chunks that contain document number and chunk number of document, both chunks assigned a computed hash value through a hash function. Then, by conducting a logical OR on these chunk values, a filter value is generated. After router received the chunk and verified the hash value, if successful hash verification, then chunk gets forwarded into next node, if unsuccessful verification then negative feedback sent upstream. Authors performed a comparison with [15] in terms of time taken from requesting phase to completed data delivery and percentage of storage overhead. The results indicate proposed mechanism is better in both parameters but held a drawback where it gives a burden to router during computation process.

The work in [105] proposed a scheme that performed an efficient content verification and have the objectives on reducing the resource wastage in verification process. Authors leverage Segmented Least Recently Used (SLRU) as a cache replacement policy. Experimental simulation performed using ns3 with self-made topology that serving content is much smaller compared to the value of cache hit-rate, due to the content store (CS) being accessed frequently to retrieve the popular contents. Result shown 90% of traffic composed of by-passing contents, despite the value of cache hit rate, with that, the large number of by-passing contents dismisses the serving contents from CS and SLRU comes to minimize the redundant verification of serving contents. SLRU divided and consists of two segments: protected and unprotected segment. LRU applies both. Mitigations of poisoned content performed when content is not poisoned and hit unprotected segment, then it moved to protected segment. This preference or verified to the content improves cache hit and greater chances of being accessed repeatedly thus aid in reducing resource waste when it comes to serving contents.

In concept, each ICN node could simply validate the provenance and integrity of each chunk due to a digital signature, allowing network caches to store only legitimate objects. Signature verification proposed in [106], motivated by work in [116] and [117] can be used to determine the cached data validity using cache hit. Objectives of the work is to prevent content poising attack with minimum overhead and as practical solutions for mitigation approach, as NDN native characteristic that employs signature verification will causes huge computational overhead [118]. Authors further their work in [107] that aims to mitigate the shortcoming of their preliminary work and identify attacks like cache pollution and content poisoning that targets cache locality by injecting fake content into the CS. Author able to perform testing and deployed it in real-world applications instead of simulations. From the standpoint of NDN, every chunk in content cache store that already been requested needs consumer verification thus every data packet within have their own digital signature that will preserve as authentic ownership of the content. Even so, adversaries might still carry out a verification attack by repeatedly requesting content in an effort to raise the probability that they will succeed. This forces routers to carry out redundant verification procedures, which in turn extends the amount of time it takes for the network to process requests.

The absence of an adequate verification mechanism in NDN is one of the key issues contributing to content poisoning attacks. Data-centric security support and other native aspects of naming in NDN architecture have considerable advantages, however name-based forwarding's scalability is a barrier. Authors in [108] proposed a secure namespace mapping (SNAMP) build on the foundations of Map-and-Encap [119] in addressing scalability concerns. ICN naming scheme utilized named for the content, there are two approaches in ICN that identify named content from its location-independent identifier: name-based routing and name resolution [120]. SNAMP first design in [121] and has gone through several revisions. In SNAMP secure namespace mapping-based solution, there are two components that are important: link object and link discovery. Link objects is a piece of named data that producer needs to associate name prefix and globally routed prefix. While link discovery is where NDNS (DNS for NDN) is queried by client for each component of the requested content. SNAMP mitigates content poisoning attack by changing how interests' packets that do not have corresponding entry being forwarded, rather of dropping an interest, the router analyses the attached link object to determine which delegation should be used to continue forwarding it. The attached link object cannot be replaced without detection since it contains the signature of the interest's owner.

Authors in [109] focused in preventing content poisoning attack by using two verification schemes, namely: user-assisted and router-cooperation. User-assisted content verification scheme used to verify content provider instead of the content itself in assuring the correctness, by doing this: emerges another threat scenario for consumer while attacker provide poisoned contents. While router-cooperation content verification scheme lets the edge routers to verify the content provider without the help of users by replacing asymmetric encryption into symmetric encryption. With the replacement of asymmetric to symmetric encryption, proposed schemes able to reduces the computing complexity. However, since routers is the main source: if attackers able to take control the routers, the transmission path will be compromised. Not only that, the huge number of verification when heavy traffic will cause extra burden to edge routers.

In ICN, the requesting side is called consumer and the provider are called publishers. As ICN focused on content rather than the host, consumer cannot determine from where the connect is retrieved. As a result, authenticity and integrity of the content became a challenge. So, one of the solutions is to employed publishers to digitally signed the requested content, there is still a potential threat to publisher in preserving the legitimate content without being poisoned. Authors in [110] proposed CCNCheck, mechanism that allows router to probabilistically check the content signatures. CCNCheck main objectives to increase availability of legitimate contents at the same time to reduce the network resources. CCNCheck does not check for all signature on all contents just verifies random subset of it. The drawbacks are the higher overhead taken by the router in the process of signature verification. In 2016, authors further their work in [111] by adding two deployment approaches that consists of network router gets divided into border and core routers that consist of two different verification probabilities, and second approach is verification probability at the border router that vary to pollution level perceived by routers.

Work in [122] propose an In-network Collaborative Verification mechanism (ICoV). In the proposed work, credibility is the underlying idea where the router performs an initial credibility check on each data packet that it receives, and follows up with a probability check based on the result. When a router sends a data packet as a response to the nodes, the router is required to include the credibility value to the data packet as an external reference. Credibility is based on two factors: internal and external evaluation. Where internal is a probability of successful verification on arrival data packet while external is from upstream routers which carried the received packet. Combining the following two results helps the router determine if the data packet is legitimate. This approach fosters collaboration amongst transmission path routers since credibility is calculated from upstream router evaluations. Data packets examined by upstream router will likely not be reviewed again by downstream routers. With that, the proposed design can reduce the content verification overhead and helps against mitigating content poisoning attack. Authors perform a comparison with CBS [106] from the impact of interest rate and impact of average poisoning rate and show that ICoV performance is effective in defending from content poisoning attack.

Authors in [112] compared their proposed scheme that utilize Hyperelliptic curve with work in [107] in terms of latency and verification overhead. The main goal of their proposed scheme is to prevent content poisoning attack in the context of NDN based Internet of Things (IoT). The adoption of an identity-based signature scheme to ensure content security and integrity in NDN networks based on IoT has been proposed as a way for protecting NDN networks based IoT. This strategy makes advantage of a small key size while still delivering the same level of security as bilinear pairing, Elliptic Curve Cryptosystems (ECC), and Rivest-Shamir-Alderman (RSA) encryption methods. The concept of hyperelliptic curves is applied in this technique to derive the values of the multiple factors. In this study, the performance of this technique in terms of cryptographic operations is compared to the performance of different CPA schemes. Because of the short key size that is used, it has been found to be effective.

In a similar manner to [112], authors in [113] proposed lightweight certificateless signature scheme in mitigating CPA in NDN-IoT networks. Authors uses Hyperelliptic Curve Discrete Logarithm Problem (HCDLP) with a security simulation/validation in "Automated Validation of Internet Security Protocols and Applications (AVISPA)." They examine two types of adversaries (i.e., Type I (A1) and Type II (A2)), each of which has a unique set of characteristics. In cryptography, A1 is a malevolent kind of adversary that is frequently referred to as an outsider attacker because it can replace a user's public key with a key that it has selected for itself, while A2 is insider attacker that can obtained master key. Proposed model consists of five entities, such as private key generator (PKGR), consumer, producer, NDN routers, and attacker. Nonetheless, the mentioned methods focus mostly on suggesting a lightweight content integrity checking by consumers that is an inherent characteristic of an NDN network.

B. CONSUMER DEPENDENT MITIGATION

Cache-based attacks such as CPA is a significant stumbling block in the widely adoption of caching in ICN. The use of misleading or fake content in a content poisoning attack has the potential to spread it throughout the network, resulting in the end user receiving poisoned content, which might potentially compromise the integrity of the content. When compared to cache poisoning attacks, content poisoning attacks are more dangerous since the malicious provider or consumer can still inflict damage even if there are no in-network caching measures in place. This is because the attackers are still present in the network. As previously mentioned, one signature verification mitigation strategy is the removal of poisoned material from a network by having the router to validate each data packet. With of the complex method, this mitigation technique places a large strain on the router. As a result of the hardware constraints, this strategy may be feasible, efficient, and lightweight; furthermore, signature verification requires key retrieval, which is time-consuming if the attack did not happen. So, here's an example of another mitigation technique called consumer-dependent method.

Authors in [16] and [118] further their previous study in [15] that aims to reduce the router overhead. Both works focused on mitigations of content poisoning in ICN caching for NDN architecture. Authors describe a consumer-feedback based rating option that allows routers to discriminate between legitimate and harmful information by proposing a lightweight content ranking algorithm for in NDN router for cached content. Content ranking algorithm aims to distinguish valid and invalid content from the observation of consumer behaviors. Although it validates each piece of content that causes overhead, it also rejects legitimate pieces of content if the valid piece of content behaves unnaturally, saving the invalid piece of content in its substitute. Each piece of information has a ranking value that ranges from 0 to 1, with 1 being the most essential piece of information on the list. Accordingly, it has been agreed that the new material will receive a ranking of zero. The position of this rank is gradually dropped because of a customer selecting the exclusion field to omit specific content from their search results. The consumer has an application that can use public keys to validate desirable content, and the consumer can define fake content. However, the NDN router needs the power to flush bogus content on its own. As in [16], author proposed adding interest-Key Binding to interest packer to bind the content name to the provider's public key. A key locator connects the interest with the provider key. The drawbacks it held is it can be time-consuming procedure for signature and PKI based verifications.

It is a major feature of NDN that it could cache data within the network, which makes it vulnerable to cache-based attacks like cache poisoning attack and cache pollution attack [123]. Mitigating this attack can help improve caching efficiency in architecture. NDN already established a mechanism to deal with multiple paths: forwarding strategies [124]. When it comes to forwarding, NDN has a stateful and adaptive forwarding plane, which changes the essential relation between routing and forwarding in the network. In NDN, the routing plane just computes routes to and from each producer and passes the information along to the forwarding plane for processing. The forwarding plane makes forwarding decisions with the help of a forwarding strategy module, and it also refreshes the forwarding table in accordance with the performance and policies. In contrast, forwarding plane in NDN unlike in the IP-networks which is not adaptive towards the environment.

With that, authors in [125] proposed adaptive forwarding strategy in NFD [95] for content poisoning detection and mitigation based on consumer feedback. Under this mechanism, consumers that detect poisoned content or receive a warning can alert upstream routers allowing changes in their forwarding tables. Author proposed two evasion strategies, ‘‘immediate failover’’ and ‘‘probe first’’. Immediate failover is to make the next hop as low priority for path transmission. While, in probe first is to keep a duplicate interest retrieved in case it is requested again. One of the drawbacks of the proposed mechanism is that it is possible that the least desired routes are the best. Furthermore, the report generated by a customer was unable to distinguish between harmful activity such as forwarding poisoned content and malicious behavior. Not only that but keeping track of all incoming requests will place an additional burden on both users and routers as well.

Author in [126] propose a Feedback-Based Content Poisoning Mitigation (FCPM) scheme in NDN, utilizing immediate failover scheme same as in [125]. In FPCM, consumer feedback used to inform upstream network in choosing alternative forwarding path same as in [125]. Proposed scheme able to detect malicious routers based on signature verification of data packets. In 2019, author in [126] proposed another scheme in mitigating content poisoning, namely: Ant Colony Algorithm Based Content Poisoning Mitigation (ACO-CPM) in NDN [127]. The ant colony optimization algorithm (ACO) can be used to find a short paths, which imitates behavior of ant colonies. ACO used in collecting security information towards all routers in the network and explore which routes need to be takes for data packet thus bypassing the malicious router. At the same time, cache store is cleaned from bogus data packets during collecting information about the path transmission. Author performed a comparison scheme with work in Router-Oriented Mitigation (ROM) [128] in three parameters metrics: content retrieval latency, legitimate content to total number of cache and good cache hit rate. The result from each metrics indicates ACO-CPM can alleviate content poisoning attack by malicious routers quickly and effective. Both ACO-CPM and ROM are centered on the concept that corrupt routers are on the path that might potentially transmit harmful content. On the other hand, both mechanisms need the routers to keep a history of old interests and let consumers to transmit one report for each data packet that receive in the routers resulting additional overhead.

Reputation-based trust approaches can assist in securing NDN environment [129], while in 2016, author in [128] presented Router-Oriented Mitigation (ROM) using the same strategy as [125], even when the routers are compromised, ROM able to provide security by eliminate it without interfering the transmission process. Reputation-based in each router is introduced, giving the process of content dissemination based on its reputations. The drawbacks of proposed method are high latency due to process of removing the compromised router during transmission and causses high traffic due to transmission divert into another route.

Author in [130] proposed reputation-based trust model in n identifying poisoned content. Proposed method identifies poisoned content by defined parameters of content popularity, negative feedback from user and user credibility. Drawbacks of proposed method in unable to ensure global security during content dissemination.

Authors in [103] performed an experimental measurement on content poisoning attack that easily causes bad affect to NDN. Author considers three attack scenarios: unregistered remote provide, multicast forwarding and best route forwarding. Unlike [125], where compromised router being removed from the network, in this experimental testing, author do not consider the case where router is malicious due to taking control of network element is hard in a real operating context. In the unregistered remote provider scenario, main goals are to exploit weakness in NDN implementation that exhibits unspecified behavior. While in multicast forwarding and best route forwarding scenario is to embed and utilize current NDN forwarder.

Authors in [131] proposed Bayesian Network Techniques (BNT) to detect any irregularity at the routers. Authors considering previous paper and reusing their topology in [103], so, it able to leverage traffic data by demonstrating performance of micro detectors and the capability of Bayesian approach in detecting CPA under different scenario. As an effort for NDN to be deployed in Internet Service provider as main infrastructure, monitoring plane that can address security threats is necessary to be implemented. Author leverage Bayesian Network (BN) technique based on probabilistic graphs that helps to establish causal linkages between measurements while dealing with uncertainty using probability theory. Firstly, author propose a list of metrics: number of interest packet (incoming and outgoing), number of PIT entries, and number at content stores. Then, from this list of metrics, micro detector is programmed to give a warning anytime metric value deviates from typical behavior. With combination of BN, anomaly detection based on NFD forwarding against CPA is implemented. Proposed scheme able to detect CPA but the drawbacks it holds are it place an additional burden on the network and large computation leads more complex, not only that, keep track of all stored metrics need high memory.

In the same year, same author proposed [103], [132] to further their scheme using Montimage Monitoring Tool (MMT) that is used for detection of CPA. Deployment of proposed scheme are managed using dockers containers in OpenStack platform. Authors focused on conducting experiments in determining the damage can be done to NDN from CPA attack, but they do not offer any recommendations in mitigation of the attack and using micro detector can lead to costly scheme. Summary of content poisoning attack can be seen in Table 2, we showcase proposed literature in strength and weakness. We may conclude from this review that every single solution has constraints, either in terms of effectiveness or implementation, and with that, a practical security architecture can be developed by effectively combining the existing schemes.

Authors in [133] proposed a reputation-based model for the mitigation of content poisoning. Proposed mechanism helps in determining the origins of the poisoned content and restricting the flow of the interest towards notorious sources thus avoiding the storage of harmful content in caches.

VI. RESEARCH CHALLENGES AND FUTURE DIRECTIONS

Different method decisions lead to different types of attack can be tackled. Content integrity and authenticity are important aspect in the deployment of NDN model. Data-centric security that utilized by NDN maintains data packets' integrity by using existing countermeasures. Named-based communication model have an impact to user privacy due to decoupling of requested data by name and the name of the data itself (parameters: timestamp, type, desired data, and more). With this, content integrity and authenticity must be verified to prevent malicious reporting of fake data and at the same time mechanisms are required to protect the user's privacy. In following part, we present research issues and discuss future research directions so that it can help to achieve security goals in the deployment of NDN. The summary of research challenges and future research directions are presented in Table 3:

A. DATA INTEGRITY

Data transferred via a network and is vulnerable to a wide range of attackers. During the transmission process, they are exposed to injection and manipulation. Data integrity is one of the most significant problems for NDN since it is essential for the right and complete data without being tampered. Two major methods have been suggested to achieve this objective. One example is the digital signature that is used in the NDN protocol. Each data packet is signed to facilitate integrity checking. Another method is to use the hash value of content as a self-certifying name.

B. CONTENT CACHING

Cache poisoning is a cache-based type attack is the main concern in NDN. The cache everything technique employed in NDN can also be harmful to the router and it may result in waste spaces, redundant data and prone to attacks like cache poisoning. In-networking caching is transparent and ''cache everything'' will open a path for an attacker to aim harms to the content provider. As a result, there are trust problems in ICN/NDN, and guaranteeing reliable data and preventing caches that give false data are both interesting research areas to pursue. Establishing trust connections between data providers, content repositories, and content requesters is an area that needs more study.

C. USER PRIVACY

Providing privacy for network entities (e.g., consumers and producers) in communication is superficial due to the lack of privacy support offered by ICN [134]. Therefore, it is necessary to examine the need for privacy concerns in NDN. According to [135], restrictive content-related information is revealed by the name prefix in ICN compared to IP, and in-network caching features provided, and data stored in PIT may disclose classified information about the identity of the consumer. For this reason, researchers should concentrate on the problems of privacy and data security in the deployment of NDN. Due to the visible content names, encrypting the names may be a suitable method to overcome this challenge; however, the drawback is that it increases processing overhead per-hop packet. Recently, blockchain-based security solutions for the NDN model have been proposed in the literature. However, blockchain and NDN integration is still an open research domain; thus, we urge

TABLE 2. Summary of content poisoning attack using signature verification mitigation technique.

Ref	Year	Architecture	Proposed Solution	Simulator	Topology	Strength(+)/Weakness(-)
[15]	2013	NDN	SSCIC DSCIC	N/A	N/A	(+) Can handle Static and dynamic content (-) No trust relationship between consumer and router where both can be compromised (-) Additional overhead to routers
[105] [106] [107]	2015 2017	NDN	Extention of SLRU	ndnSIM	Self-made	(+) Reduce the verification frequency thus reduce in computational overhead (-) Risk to content pollution (-) Only relies on verification
[108]	2015	NDN	Secure Namespace	ndnSIM	Replicated at Terabits and UCLA Computer Science Department	(-) Cannot handle if routers is malicious (-) Scalability problem
[109]	2017	NDN	Self-certifying Hash function	Microsoft Visual C++	N/A	(-) High latency (-) Reduce throughput of of the network (-) Verification process will be a burden to edge routers to performed
[110], [111]	2014	CCN	CCNCheck Probability Check	NS3	Rocketfuel topology	(-) Hard to find the optimal probabilistic value
[112]	2020	NDN	Identity-based signature schemes	AVISPA	Smart city topology	(+) Low latency (+) Less verification overhead. (-) Complex process
[113]	2021	NDN	Identity-based signature schemes	AVISPA	NDN-IoT	(-) Requires third-party to produce and deliver the participants' secret key

TABLE 3. Security challanges and future research directions.

Aspects	Challenges	Future potential directions
Data Integrity	Determining the encryption keys that will be used in data distribution. Ensuring content legitimacy from legitimate producer.	Securing method using self-certifying naming mechanism. Lightweight signature verification and generation. With the hash value of the content as a self-certifying identifier.
Content caching	Redundancy of "cache everything everywhere". Cache store pollution. Pending Interest Table poisoning. Transparent caching poses security issues for producers. No efficient and robust cache freshness mechanism.	Establish caching policy deciding content needed to be cache, and duration of it being stored. Verification of content and producers using blockchain technology Caching strategy for freshness in mitigating replay attack.
User Privacy	Content name can be used to detect identity of user. Timing attack on cache privacy.	Encrypted naming mechanism. Privacy preserving using blockchain technology. Anonymous communication channel.
Access Control	Content cached at routers easily accessible. Access control policy for routers and cache store.	Attribute-Based Encryption to protect the data. Models for scalability in key distribution and trust management
Digital Signature	It is necessary to develop a mechanism that allows routers to efficiently verify the signature of the packet at line speed. Take into account all potential attacker that can be router, producer or compromised router and approaches mechanism to mitigate integrity attack should take into account all of the potential attacker. Routers should be able to limit the amount of signatures that need to be examined by using signature mitigation techniques.	Encryption techniques that are both lightweight and resource-conserving Elliptic curve encryption that has a lower degree of complexity

further research to explore the benefits and challenges of blockchain-based security solutions in NDN.

D. ACCESS CONTROL

Due to the lack of hosts and the widespread use of caching, traditional defenses are not particularly effective against ICN attacks. Thus, to provide data integrity, a flexible and adequate access control system must be implemented. How can access to material that has been extensively cached at routers be controlled?, it is possible to address this issue using Attribute-Based Encryption (ABE) proposed before. Control policies may be thought of as characteristics that help to safeguard information.

E. DIGITAL SIGNATURE

ICN comes with built-in security, unlike IP, which relies on the upper layers to secure host-to-host communication. In ICN, the content itself is readily shared along with the producer's signature key that is used to verify the integrity of received content. To be more particular, the security in ICN complies to a concept that is data-centric. As a result, the content has been digitally signed by the content provider so that interested senders can validate its integrity and identify where the data originated from. Therefore, to adapt to the newly built network, it asks for a signature method that is more efficient than conventional ones. Signature creation and verification must be very efficient to achieve high speed networking. Also urgently needed are studies and standards for efficient post-quantum computer digital signature systems, which are now under development.

F. BLOCKCHAIN

The developing concept of Blockchain technology in the NDN is making its way forward quickly. Blockchain technology over IP is still troubled by major issues, such as a lack of performance for hierarchical access and a lack of security. The adoption of blockchain technology over NDN has resolved these issues by offering a decentralized system while also simplifying the architecture of the NDN network. To trace and secure data transmission among objects, it is necessary to record data transactions between pairings of objects to do so. According to the security analysis, the proposed blockchain framework in [85] achieves encryption in milliseconds and blockchain operation in several seconds for data sharing, allowing it to adapt to the NDN of things in a secure and efficient manner while maintaining high performance. In NDN-based blockchain technology, users can name the data as well as the keys used to encrypt the data. Each packet is protected against being read as it travels via the network owing to an encrypted signature. Distributed solutions based on blockchain technology can be used to enforce the binding of content names and preserve the privacy of both the user and the content [136].

The ICN paradigm provides researchers with the chance to integrate security into the foundation of the Internet and could figure out what may work and what is not in the conventional Internet architecture to improve security. Nevertheless, providing a secure solution and protecting the network will always be a never-ending process, as new threats emerge, new attacks are investigated and new security solutions are introduced. Researchers will be able to offer better and faster countermeasures if they start with secure and consolidated security foundations that are built into the architecture. As a result, the Internet will become a much more secure environment.

VII. CONCLUSION

NDN is suitable candidate architecture for replacing TCP/IP and has potential to be integrated in IoT applications, it offers great security features and data distribution. In this paper, we have introduced the attacks on content integrity and authenticity in ICN. We have potential attack on both content integrity and authenticity including the existing countermeasures against it. In the future, we will look at a different aspects of security goals like privacy that will be affected by naming characteristics in ICN. Despite considerable progress of research in NDN technology, there are still some issues that need to be resolved and we hope that this conception can provide an insight to researchers on attacks in NDN and its countermeasures and will help identify a new strategy in tackling vulnerabilities mentioned and come out with new mitigations techniques.

REFERENCES

[1] D. P. Arjunwadkar, "Introduction of NDN with comparison to current internet architecture based on TCP/IP," *Int. J. Comput. Appl.*, vol. 105, no. 5, pp. 1–5, 2014.

[2] J. Liang, J. Jiang, H. Duan, K. Li, T. Wan, and J. Wu, "When HTTPS meets CDN: A case of authentication in delegated service," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 67–82, doi: 10.1109/SP.2014.12.

[3] A. Passarella, "A survey on content-centric technologies for the current internet: CDN and P2P solutions," *Comput. Commun.*, vol. 35, no. 1, pp. 1–32, Jan. 2012. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0140366411003173, doi: 10.1016/j.comcom.2011.10.005.

[4] G. Pallis and A. Vakali, "Content delivery networks," *Commun. ACM*, vol. 49, no. 1, p. 101, 2006.

[5] G. Ma, Z. Chen, J. Cao, Z. Guo, Y. Jiang, and X. Guo, "A tentative comparison on CDN and NDN," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2014, pp. 2893–2898. [Online]. Available: https://ieeexplore.ieee.org/document/6974369, doi: 10.1109/SMC.2014.6974369.

[6] *Cisco Annual Internet Report—Cisco Annual Internet Report (2018–2023) White Paper*. Accessed: Jun. 12, 2022. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[7] V. Jacobson, D. K. Smetters, J. D. Thornton, M. Plass, N. Briggs, and R. Braynard, "Networking named content," *Commun. ACM*, vol. 55, no. 1, pp. 117–124, Jan. 2012. [Online]. Available: https://dl.acm.org/doi/10.1145/2063176.2063204, doi: 10.1145/2063176.2063204.

[8] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. D. Thornton, D. K. Smetters, B. Zhang, G. Tsudik, D. Massey, and C. Papadopoulos, "Named data networking (NDN) project," Xerox Palo Alto Res. Center, Palo Alto, CA, USA, Tech. Rep. NDN-0001, PARC 157, 158, 2010.

[9] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," *IEEE Commun. Mag.*, vol. 50, no. 7, pp. 26–36, Jul. 2012. [Online]. Available: http://ieeexplore.ieee.org/document/6231276/, doi: 10.1109/MCOM.2012.6231276.

[10] X. Fu, D. Kutscher, S. Misra, and R. Li, "Information-centric networking security," *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 60–61, Nov. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8539022/, doi: 10.1109/MCOM.2018.8539022.

[11] D. Kutscher, S. Eum, K. Pentikousis, I. Psaras, D. Corujo, D. Saucez, T. Schmidt, and M. Waehlisch, *Information-Centric Networking (ICN) Research Challenges*, document RFC 7927, RFC Editor, Jul. 2016. [Online]. Available: https://www.rfc-editor.org/info/rfc7927, doi: 10.17487/RFC7927.

[12] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, K. Claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 66–73, 2014, doi: 10.1145/2656877.2656887.

[13] W. Wong and P. Nikander, "Secure naming in information-centric networks," in *Proc. Re-Architecting Internet Workshop*. Philadelphia, PA, USA: ACM Press, Nov. 2010, p. 1. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1921233.1921248, doi: 10.1145/1921233.1921248.

[14] X. Zhang, K. Chang, H. Xiong, Y. Wen, G. Shi, and G. Wang, "Towards name-based trust and security for content-centric network," in *Proc. 19th IEEE Int. Conf. Netw. Protocols*, Oct. 2011, pp. 1–6, doi: 10.1109/ICNP.2011.6089053.

[15] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "DoS and DDoS in named data networking," in *Proc. 22nd Int. Conf. Comput. Commun. Netw. (ICCCN)*, Nassau, Bahamas, Jul. 2013, pp. 1–7. [Online]. Available: http://ieeexplore.ieee.org/document/6614127/, doi: 10.1109/ICCCN.2013.6614127.

[16] C. Ghali, G. Tsudik, and E. Uzun, "Network-layer trust in named-data networking," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 5, pp. 12–19, Oct. 2014. [Online]. Available: https://dl.acm.org/doi/10.1145/2677046.2677049, doi: 10.1145/2677046.2677049.

[17] G. Tyson, N. Sastry, I. Rimac, R. Cuevas, and A. Mauthe, "A survey of mobility in information-centric networks: Challenges and research directions," in *Proc. 1st ACM workshop Emerg. Name-Oriented Mobile Netw. Design Archit., Algorithms, Appl.* Hilton Head, CA, USA: ACM Press, Jun. 2012, pp. 1–6. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2248361.2248363, doi: 10.1145/2248361.2248363.

[18] A. Afanasyev, J. Burke, T. Refaei, L. Wang, B. Zhang, and L. Zhang, "A brief introduction to named data networking," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Los Angeles, CA, USA, Oct. 2018, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/8599682/, doi: 10.1109/MILCOM.2018.8599682.

[19] D. Saxena, V. Raychoudhury, N. Suri, C. Becker, and J. Cao, "Named data networking: A survey," *Comput. Sci. Rev.*, vol. 19, pp. 15–55, Feb. 2016. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1574013715300599, doi: 10.1016/j.cosrev.2016.01.001.

[20] E. G. Abdallah, H. S. Hassanein, and M. Zulkernine, "A survey of security attacks in information-centric networking," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1441–1454, 3rd Quart., 2015. [Online]. Available: http://ieeexplore.ieee.org/document/7009958/, doi: 10.1109/COMST.2015.2392629.

[21] R. Tourani, T. Mick, S. Misra, and G. Panwar, "Security, privacy, and access control in information-centric networking: A survey," Jun. 2017, *arXiv:1603.03409*.

[22] T. Chatterjee, S. Ruj, and S. D. Bit, "Security issues in named data networks," *Computer*, vol. 51, no. 1, pp. 66–75, Jan. 2018. [Online]. Available: http://ieeexplore.ieee.org/document/8267994/, doi: 10.1109/MC.2018.1151010.

[23] E. Mannes and C. Maziero, "Naming content on the network layer: A security analysis of the information-centric network model," *ACM Comput. Surv.*, vol. 52, no. 3, pp. 1–28, May 2020. [Online]. Available: https://dl.acm.org/doi/10.1145/3311888, doi: 10.1145/3311888.

[24] N. Kumar, A. K. Singh, A. Aleem, and S. Srivastava, "Security attacks in named data networking: A review and research directions," *J. Comput. Sci. Technol.*, vol. 34, no. 6, pp. 1319–1350, Nov. 2019. [Online]. Available: http://link.springer.com/10.1007/s11390-019-1978-9, doi: 10.1007/s11390-019-1978-9.

[25] S. Rai and D. Dhakal, "A survey on detection and mitigation of interest flooding attack in named data networking," in *Advanced Computational and Communication Paradigms*. Singapore: Springer, 2018, pp. 523–531, doi: 10.1007/978-981-10-8237-5_51.

[26] R.-T. Lee, Y.-B. Leau, Y. J. Park, and M. Anbar, "A survey of interest flooding attack in named-data networking: Taxonomy, performance and future research challenges," *IETE Tech. Rev.*, vol. 39, no. 5, pp. 1027–1045, Sep. 2022, doi: 10.1080/02564602.2021.1957029.

[27] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest flooding attack and countermeasures in named data networking," in *Proc. IFIP Netw. Conf.*, 2013, pp. 1–9.

[28] N. Chhetry and H. K. Kalita, "Interest flooding attack in named data networking: A survey," Dept. Inf. Technol., North Eastern Hill Univ., Shillong, India, Mar. 2016.

[29] R. A. Rehman. (2019). *Interest Flooding Attack Mitigation in Named Data Networking Based VANETs*. [Online]. Available: https://www.academia.edu/42259014/Interest_Flooding_Attack_Mitigation_in_Named_Data_Networking_based_VANETs

[30] N. A. Tumpa, "Mitigating DDoS attack in named data network," 2019. Accessed: Nov. 27, 2021. [Online]. Available: http://lib.buet.ac.bd:8080/xmlui/handle/123456789/5821

[31] A. Mohaisen, H. Mekky, X. Zhang, H. Xie, and Y. Kim, "Timing attacks on access privacy in information centric networks and countermeasures," *IEEE Trans. Depend. Sec. Comput.*, vol. 12, no. 6, pp. 675–687, Nov. 2015, doi: 10.1109/TDSC.2014.2382592.

[32] A. Chaabane, E. De Cristofaro, M.-A. Kaafar, and E. Uzun, "Privacy in content-oriented networking: Threats and countermeasures," Jul. 2013, *arXiv:1211.5183*.

[33] J. Rexford and C. Dovrolis, "Future internet architecture: Clean-slate versus evolutionary research," *Commun. ACM*, vol. 53, no. 9, pp. 36–40, Sep. 2010.

[34] D. Cheriton and M. Gritter, "TRIAD: A new next-generation internet architecture," ResearchGate, Dept. Comput. Sci., Stanford Univ., Jan. 2000.

[35] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica, "A data-oriented (and beyond) network architecture," in *Proc. Conf. Appl., Technol., Architectures, Protocols Comput. Commun.* New York, NY, USA: Association for Computing Machinery, Aug. 2007, pp. 181–192, doi: 10.1145/1282380.1282402.

[36] *NSF Future Internet Architecture Project*. Accessed: Jun. 13, 2022. [Online]. Available: http://www.nets-fia.net/

[37] M. Ambrosin, A. Compagno, M. Conti, C. Ghali, and G. Tsudik, "Security and privacy analysis of national science foundation future internet architectures," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1418–1442, 2nd Quart., 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8269274/, doi: 10.1109/COMST.2018.2798280.

[38] I. Seskar, K. Nagaraja, S. Nelson, and D. Raychaudhuri, "MobilityFirst future internet architecture project," in *Proc. 7th Asian Internet Eng. Conf.* New York, NY, USA: Association for Computing Machinery, Nov. 2011, pp. 1–3, doi: 10.1145/2089016.2089017.

[39] D. Lagutin, K. Visala, and S. Tarkoma, "Publish/subscribe for internet: PSIRP perspective," in *Towards the Future Internet*. Amsterdam, The Netherlands: IOS Press, 2010, pp. 75–84. [Online]. Available: https://ebooks.iospress.nl/doi/10.3233/978-1-60750-539-6-75, doi: 10.3233/978-1-60750-539-6-75.

[40] N. Fotiou, P. Nikander, D. Trossen, and G. C. Polyzos, "Developing information networking further: From PSIRP to PURSUIT," in *Broadband Communications, Networks, and Systems* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 66, I. Tomkos, C. J. Bouras, G. Ellinas, P. Demestichas, and P. Sinha, Eds. Berlin, Germany: Springer, 2012, pp. 1–13, [Online]. Available: http://link.springer.com/10.1007/978-3-642-30376-0_1, doi: 10.1007/978-3-642-30376-0_1.

[41] *PSIRP | PSIRP*. Accessed: Jun. 13, 2022. [Online]. Available: http://www.psirp.org/

[42] C. Dannewitz, D. Kutscher, B. Ohlman, S. Farrell, B. Ahlgren, and H. Karl, "Network of information (NetInf)—An information-centric networking architecture," *Comput. Commun.*, vol. 36, no. 7, pp. 721–735, Apr. 2013. Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0140366413000364, doi: 10.1016/j.comcom.2013.01.009.

[43] *The Convergence Project*. Accessed: Jun. 13, 2022. [Online]. Available: http://www.ict-convergence.eu/

[44] *SAIL*. Accessed: Jun. 13, 2022. [Online]. Available: https://www.sail-project.eu/

[45] *COMET Project Website*. Accessed: Jun. 13, 2022. [Online]. Available: http://www.comet-project.org/

[46] M. S. M. Shah, Y.-B. Leau, Z. Yan, and M. Anbar, "Hierarchical naming scheme in named data networking for Internet of Things: A review and future security challenges," *IEEE Access*, vol. 10, pp. 19958–19970, 2022, doi: 10.1109/ACCESS.2022.3151864.

[47] A. Ghodsi, T. Koponen, J. Rajahalme, P. Sarolahti, and S. Shenker, "Naming in content-oriented architectures," in *Proc. ACM SIGCOMM Workshop Inf.-Centric Netw.* Toronto, ON, Canada: ACM Press, Aug. 2011, pp. 1–6. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2018584.2018586, doi: 10.1145/2018584.2018586.

[48] F. Li, F. Chen, J. Wu, and H. Xie, "Longest prefix lookup in named data networking: How fast can it be?" in *Proc. 9th IEEE Int. Conf. Netw., Archit., Storage*, Tianjin, China, Aug. 2014, pp. 186–190. [Online]. Available: http://ieeexplore.ieee.org/document/6923179/, doi: 10.1109/NAS.2014.36.

[49] Z. Ullah, M. I. U. Haq, S. Khan, and M. Zubair, "DSAC-digital signature for access control in information centric network," Univ. Agricult., Peshawar, Pakistan, Sep. 2021, doi: 10.20944/preprints202105.0179.v2.

[50] N. Fotiou and G. C. Polyzos, "Enabling NAME-based security and trust," in *Trust Management IX* (IFIP Advances in Information and Communication Technology), C. D. Jensen, S. Marsh, T. Dimitrakos, and Y. Murayama, Eds. Cham, Switzerland: Springer, Cham, 2015, pp. 47–59, doi: 10.1007/978-3-319-18491-3_4.

[51] Z. Shah, I. Ullah, H. Li, A. Levula, and K. Khurshid, "Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey," *Sensors*, vol. 22, no. 3, p. 1094, Jan. 2022.

[52] A. Djama, B. Djamaa, and M. R. Senouci, "Information-centric networking solutions for the Internet of Things: A systematic mapping review," *Comput. Commun.*, vol. 159, pp. 37–59, Jun. 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0140366419316901, doi: 10.1016/j.comcom.2020.05.003.

[53] S. Arshad, M. A. Azam, M. H. Rehmani, and J. Loo, "Recent advances in information-centric networking-based Internet of Things (ICN-IoT)," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2128–2158, Apr. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8478349/, doi: 10.1109/JIOT.2018.2873343.

[54] D. Mars, S. M. Gammar, A. Lahmadi, and L. A. Saidane, "Using information centric networking in Internet of Things: A survey," *Wireless Pers. Commun.*, vol. 105, no. 1, pp. 87–103, 2019. [Online]. Available: http://link.springer.com/10.1007/s11277-018-6104-8, doi: 10.1007/s11277-018-6104-8.

[55] A. Aboodi, T.-C. Wan, and G.-C. Sodhy, "Survey on the incorporation of NDN/CCN in IoT," *IEEE Access*, vol. 7, pp. 71827–71858, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8726307/, doi: 10.1109/ACCESS.2019.2919534.

[56] B. Nour, K. Sharif, F. Li, S. Biswas, H. Moungla, M. Guizani, and Y. Wang, "A survey of Internet of Things communication using ICN: A use case perspective," *Comput. Commun.*, vols. 142–143, pp. 95–123, Jun. 2019. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0140366418309228

[57] M. Amadeo, C. Campolo, J. Quevedo, D. Corujo, A. Molinaro, A. Iera, R. L. Aguiar, and A. V. Vasilakos, "Information-centric networking for the Internet of Things: Challenges and opportunities," *IEEE Netw.*, vol. 30, no. 2, pp. 92–100, Mar. 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7437030/, doi: 10.1109/MNET.2016.7437030.

[58] W. M. Kiruba and M. Vijayalakshmi, "Implementation and analysis of data security in a real time IoT based healthcare application," in *Proc. 2nd Int. Conf. Trends Electron. Informat. (ICOEI)*, May 2018, pp. 1460–1465, doi: 10.1109/ICOEI.2018.8553908.

[59] D. Saxena, V. Raychoudhury, and N. SriMahathi, "SmartHealth-NDNoT: Named data network of things for healthcare services," in *Proc. MobileHealth@ MobiHoc*, Jun. 2015, pp. 45–50, doi: 10.1145/2757290.2757300.

[60] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2027–2051, 3rd Quart., 2016, doi: 10.1109/COMST.2016.2548426.

[61] N. Fotiou and G. C. Polyzos, "Name-based security for information-centric networking architectures," *Future Internet*, vol. 11, no. 11, p. 232, Nov. 2019. [Online]. Available: https://www.mdpi.com/1999-5903/11/11/232, doi: 10.3390/fi11110232.

[62] N. Fotiou and B. A. Alzahrani, "Rendezvous-based access control for information-centric architectures," *Int. J. Netw. Manage.*, vol. 28, no. 1, Jan. 2018, Art. no. e2007. [Online]. Available: http://doi.wiley.com/10.1002/nem.2007, doi: 10.1002/nem.2007.

[63] Q. Li, X. Zhang, Q. Zheng, R. Sandhu, and X. Fu, "LIVE: Lightweight integrity verification and content access control for named data networking," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 308–320, Feb. 2015, doi: 10.1109/TIFS.2014.2365742.

[64] Q. Li, P. P. C. Lee, P. Zhang, P. Su, L. He, and K. Ren, "Capability-based security enforcement in named data networking," *IEEE/ACM Trans. Netw.*, vol. 25, no. 5, pp. 2719–2730, Oct. 2017, doi: 10.1109/TNET.2017.2715822.

[65] Y. Fan, Y. Tao, and Y. Zhu, "A lightweight verification mechanism for MPEG-DASH in named data networking," in *Proc. 3rd Int. Conf. Hot Inf.-Centric Netw. (HotICN)*, Hefei, China, Dec. 2020, pp. 102–107. [Online]. Available: https://ieeexplore.ieee.org/document/9350751/, doi: 10.1109/HotICN50779.2020.9350751.

[66] P. He, Y. Wan, Q. Xia, S. Li, J. Hong, and K. Xue, "LASA: Lightweight, auditable and secure access control in ICN with limitation of access times," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kansas City, MO, USA, 2018, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/8422829/, doi: 10.1109/ICC.2018.8422829.

[67] Z. Song and P. Kar, "Name-signature lookup system: A security enhancement to named data networking," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Guangzhou, China, Dec. 2020, pp. 1444–1448. [Online]. Available: https://ieeexplore.ieee.org/document/9343242/, doi: 10.1109/TrustCom50675.2020.00194.

[68] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2009, pp. 911–918, doi: 10.1109/ALLERTON.2009.5394956.

[69] W. Shang, Q. Ding, A. Marianantoni, J. Burke, and L. Zhang, "Securing building management systems using named data networking," *IEEE Netw.*, vol. 28, no. 3, pp. 50–56, May/Jun. 2014. [Online]. Available: http://ieeexplore.ieee.org/document/6843232/, doi: 10.1109/MNET.2014.6843232.

[70] S. Adhikari, S. Ray, M. S. Obaidat, and G. P. Biswas, "Efficient and secure content dissemination architecture for content centric network using ECC-based public key infrastructure," *Comput. Commun.*, vol. 157, pp. 187–203, May 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0140366419310771, doi: 10.1016/j.comcom.2020.04.024.

[71] K. Asaf, R. A. Rehman, and B.-S. Kim, "Blockchain technology in named data networks: A detailed survey," *J. Netw. Comput. Appl.*, vol. 171, Dec. 2020, Art. no. 102840. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804520303088, doi: 10.1016/j.jnca.2020.102840.

[72] J. Guo, M. Wang, B. Chen, S. Yu, H. Zhang, and Y. Zhang, "Enabling blockchain applications over named data networking," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6, doi: 10.1109/ICC.2019.8761919.

[73] S. Mori, "Secure caching scheme by using blockchain for information-centric network-based wireless sensor networks," *J. Signal Process.*, vol. 22, no. 3, pp. 97–108, May 2018, doi: 10.2299/jsp.22.97.

[74] J. Lou, Q. Zhang, Z. Qi, and K. Lei, "A blockchain-based key management scheme for named data networking," in *Proc. 1st IEEE Int. Conf. Hot Inf.-Centric Netw. (HotICN)*, Aug. 2018, pp. 141–146, doi: 10.1109/HOTICN.2018.8605993.

[75] N. Anita and V. Murugesan, "IoT security in supply chain using blockchain," in *Proc. 2nd Int. Conf. Commun., Comput. Ind. 4.0 (C2I4)*, Dec. 2021, pp. 1–6, doi: 10.1109/C2I454156.2021.9689263.

[76] B. Li, D. Huang, Z. Wang, and Y. Zhu, "Attribute-based access control for ICN naming scheme," *IEEE Trans. Depend. Sec. Comput.*, vol. 15, no. 2, pp. 194–206, Mar. 2018. [Online]. Available: http://ieeexplore.ieee.org/document/7447763/, doi: 10.1109/TDSC.2016.2550437.

[77] C. Ghali, M. A. Schlosberg, G. Tsudik, and C. A. Wood, "Interest-based access control for content centric networks," in *Proc. 2nd ACM Conf. Inf.-Centric Netw.* New York, NY, USA: Association for Computing Machinery, Sep. 2015, pp. 147–156, doi: 10.1145/2810156.2810174.

[78] J. Kurihara, K. Yokota, and A. Tagami, "A consumer-driven access control approach to censorship circumvention in content-centric networking," in *Proc. 3rd ACM Conf. Inf.-Centric Netw.*, Sep. 2016, pp. 186–194, doi: 10.1145/2984356.2984360.

[79] E. G. Abdallah, M. Zulkernine, and H. S. Hassanein, "DACPI: A decentralized access control protocol for information centric networking," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6, doi: 10.1109/ICC.2016.7511198.

[80] S. Adhikari and S. Ray, "A lightweight and secure IoT communication framework in content-centric network using elliptic curve cryptography," in *Recent Trends in Communication, Computing, and Electronics* (Lecture Notes in Electrical Engineering), vol. 524, A. Khare, U. S. Tiwary, I. K. Sethi, and N. Singh, Eds. Singapore: Springer, 2019, pp. 207–216. [Online]. Available: http://link.springer.com/10.1007/978-981-13-2685-1_21, doi: 10.1007/978-981-13-2685-1_21.

[81] J. Burke, P. Gasti, N. Nathan, and G. Tsudik, "Securing instrumented environments over content-centric networking: The case of lighting control and NDN," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Turin, Italy, Apr. 2013, pp. 394–398. [Online]. Available: http://ieeexplore.ieee.org/document/6970725/, doi: 10.1109/INFCOMW.2013.6970725.

[82] T. Li, J. Liang, L. Geng, and Y. Liu, "A privacy-preserving scheme based on fragments storage and fragments recombination in CCN," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2019, pp. 1–6, doi: 10.1109/ISCC47284.2019.8969757.

[83] K. T. Ko, H. H. Hlaing, and M. Mambo, "A PEKS-based NDN strategy for name privacy," *Future Internet*, vol. 12, no. 8, p. 130, Jul. 2020. [Online]. Available: https://www.mdpi.com/1999-5903/12/8/130, doi: 10.3390/fi12080130.

[84] K. Xu, Y. Wan, and G. Xue, "Powering smart homes with information-centric networking," *IEEE Commun. Mag.*, vol. 57, no. 6, pp. 40–46, Jun. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8740791/, doi: 10.1109/MCOM.2019.1800732.

[85] K. Zhu, Z. Chen, W. Yan, and L. Zhang, "Security attacks in named data networking of things and a blockchain solution," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4733–4741, Jun. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8502794/, doi: 10.1109/JIOT.2018.2877647.

[86] M. Conti, M. Hassan, and C. Lal, "BlockAuth: BlockChain based distributed producer authentication in ICN," *Comput. Netw.*, vol. 164, Dec. 2019, Art. no. 106888. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128619308308, doi: 10.1016/j.comnet.2019.106888.

[87] R. S. da Silva and S. D. Zorzo, "An access control mechanism to ensure privacy in named data networking using attribute-based encryption with immediate revocation of privileges," in *Proc. 12th Annu. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, Jan. 2015, pp. 128–133. [Online]. Available: http://ieeexplore.ieee.org/document/7157958/, doi: 10.1109/CCNC.2015.7157958.

[88] R. Tourani, S. Misra, J. Kliewer, S. Ortegel, and T. Mick, "Catch me if you can: A practical framework to evade censorship in information-centric networks," in *Proc. 2nd ACM Conf. Inf.-Centric Netw.*, San Francisco CA, USA, Sep. 2015, pp. 167–176. [Online]. Available: https://dl.acm.org/doi/10.1145/2810156.2810171, doi: 10.1145/2810156.2810171.

[89] B. Nour, H. Khelifi, R. Hussain, S. Mastorakis, and H. Moungla, "Access control mechanisms in named data networks: A comprehensive survey," 2020, *arXiv:2012.04624*.

[90] R. Boussada, B. Hamdaney, M. E. Elhdhili, S. Argoubi, and L. A. Saidane, "A secure and privacy-preserving solution for IoT over NDN applied to E-health," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018, pp. 817–822. [Online]. Available: https://ieeexplore.ieee.org/document/8450374/, doi: 10.1109/IWCMC.2018.8450374.

[91] S. DiBenedetto, P. Gasti, G. Tsudik, and E. Uzun, "ANDaNA: Anonymous named data networking application," Jan. 2012, *arXiv:1112.2205*.

[92] R. Boussada, B. Hamdane, M. E. Elhdhili, and L. A. Saidane, "PP-NDNoT: On preserving privacy in IoT-based E-health systems over NDN," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Marrakesh, Morocco, Apr. 2019, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/8886110/, doi: 10.1109/WCNC.2019.8886110.

[93] Aroosa, S. S. Ullah, S. Hussain, R. Alroobaea, and I. Ali, "Securing NDN-based Internet of Health Things through cost-effective signcryption scheme," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–13, Apr. 2021. [Online]. Available: https://www.hindawi.com/journals/wcmc/2021/5569365/, doi: 10.1155/2021/5569365.

[94] Z. Zhang, S. Liu, R. King, and L. Zhang, "Supporting multiparty signing over named data networking," Jun. 2021, *arXiv:2106.04030*.

[95] A. Afanasyev, J. Shi, B. Zhang, L. Zhang, I. Moiseenko, Y. Yu, W. Shang, Y. Huang, J. P. Abraham, and S. DiBenedetto, "NFD developer's guide," Univ. California, Los Angeles, CA, USA, Tech. Rep. NDN-0021, 2016. [Online]. Available: http://named-data.net/wp-content/uploads/2014/07/NFD-developer-guide.pdf

[96] Y. Yu, Y. Li, X. Du, R. Chen, and B. Yang, "Content protection in named data networking: Challenges and potential solutions," *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 82–87, Nov. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8539026/, doi: 10.1109/MCOM.2018.1701086.

[97] Q. T. Thai, N. Ko, S. H. Byun, and S.-M. Kim, ''Design and implementation of NDN-based Ethereum blockchain,'' *J. Netw. Comput. Appl.*, vol. 200, Apr. 2022, Art. no. 103329. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804521003143, doi: 10.1016/j.jnca.2021.103329.

[98] X. Li, Y. Mei, J. Gong, F. Xiang, and Z. Sun, ''A blockchain privacy protection scheme based on ring signature,'' *IEEE Access*, vol. 8, pp. 76765–76772, 2020, doi: 10.1109/ACCESS.2020.2987831.

[99] N. Kumar, A. Aleem, A. K. Singh, and S. Srivastava, ''NBP: Namespace-based privacy to counter timing-based attack in named data networking,'' *J. Netw. Comput. Appl.*, vol. 144, pp. 155–170, Oct. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804519302280, doi: 10.1016/j.jnca.2019.07.004.

[100] A. M. Qureshi, N. Anjum, R. N. B. Rais, M. Ur-Rehman, and A. Qayyum, ''Detection of malicious consumer interest packet with dynamic threshold values,'' *PeerJ Comput. Sci.*, vol. 7, p. e435, Mar. 2021. [Online]. Available: https://peerj.com/articles/cs-435, doi: 10.7717/peerj-cs.435.

[101] T. Lauinger, ''Security & scalability of content-centric networking,'' M.S. thesis, TU Darmstadt, Darmstadt, Germany, 2010.

[102] C. Fang, H. Yao, Z. Wang, W. Wu, X. Jin, and F. R. Yu, ''A survey of mobile information-centric networking: Research issues and challenges,'' *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2353–2371, 3rd Quart., 2018, doi: 10.1109/COMST.2018.2809670.

[103] T. Nguyen, X. Marchal, G. Doyen, T. Cholez, and R. Cogranne, ''Content poisoning in named data networking: Comprehensive characterization of real deployment,'' in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM)*, May 2017, pp. 72–80, doi: 10.23919/INM.2017.7987266.

[104] L. Wang, A. Hoque, C. Yi, A. Alyyan, and B. Zhang, ''OSPFN: An OSPF based routing protocol for named data networking,'' NDN Project, Tech. Rep. NDN-0003, 2012. [Online]. Available: https://named-data.net/publications/techreports/trospfn/

[105] S. Nam, D. Kim, and I. Yeom, ''Content verification in named data networking,'' in *Proc. Int. Conf. Inf. Netw. (ICOIN)*. Washington, DC, USA: IEEE Computer Society, Jan. 2015, pp. 414–415. [Online]. Available: https://www.computer.org/csdl/proceedings-article/icoin/2015/07057931/12OmNx1Iwg4, doi: 10.1109/ICOIN.2015.7057931.

[106] D. Kim, S. Nam, J. Bi, and I. Yeom, ''Efficient content verification in named data networking,'' in *Proc. 2nd ACM Conf. Inf.-Centric Netw.*, San Francisco, CA, USA, Sep. 2015, pp. 109–116. [Online]. Available: https://dl.acm.org/doi/10.1145/2810156.2810165, doi: 10.1145/2810156.2810165.

[107] D. Kim, J. Bi, A. V. Vasilakos, and I. Yeom, ''Security of cached content in NDN,'' *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 12, pp. 2933–2944, Dec. 2017, doi: 10.1109/TIFS.2017.2725229.

[108] A. Afanasyev, C. Yi, L. Wang, B. Zhang, and L. Zhang, ''SNAMP: Secure namespace mapping to scale NDN forwarding,'' in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Hong Kong, Apr. 2015, pp. 281–286. [Online]. Available: http://ieeexplore.ieee.org/document/7179398/, doi: 10.1109/INFCOMW.2015.7179398.

[109] Y. Wang, Z. Qi, K. Lei, B. Liu, and C. Tian, ''Preventing 'bad' content dispersal in named data networking,'' in *Proc. ACM Turing 50th Celebration Conf. China*. New York, NY, USA: Association for Computing Machinery, May 2017, pp. 1–8, doi: 10.1145/3063955.3063993.

[110] I. Ribeiro, A. Rocha, C. Albuquerque, and F. Guimaraes, ''On the possibility of mitigating content pollution in content-centric networking,'' in *Proc. 39th Annu. IEEE Conf. Local Comput. Netw.*, Sep. 2014, pp. 498–501, doi: 10.1109/LCN.2014.6925826.

[111] I. Ribeiro, A. Rocha, C. Albuquerque, and F. Guimarães, ''Content pollution mitigation for content-centric networking,'' in *Proc. 7th Int. Conf. Netw. Future (NOF)*, Nov. 2016, pp. 1–5, doi: 10.1109/NOF.2016.7810123.

[112] S. S. Ullah, I. Ullah, H. Khattak, M. A. Khan, M. Adnan, S. Hussain, N. U. Amin, and M. A. K. Khattak, ''A lightweight identity-based signature scheme for mitigation of content poisoning attack in named data networking with Internet of Things,'' *IEEE Access*, vol. 8, pp. 98910–98928, 2020, doi: 10.1109/ACCESS.2020.2995080.

[113] S. Hussain, S. S. Ullah, A. Gumaei, M. Al-Rakhami, I. Ahmad, and S. M. Arif, ''A novel efficient certificateless signature scheme for the prevention of content poisoning attack in named data networking-based Internet of Things,'' *IEEE Access*, vol. 9, pp. 40198–40215, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9367230/, doi: 10.1109/ACCESS.2021.3063490.

[114] D. Mazières, M. Kaminsky, M. F. Kaashoek, and E. Witchel, ''Separating key management from file system security,'' in *Proc. 17th ACM Symp. Operating Syst. Princ.* New York, NY, USA: Association for Computing Machinery, Dec. 1999, pp. 124–139, doi: 10.1145/319151.319160.

[115] S. Srinivasan and A. P. Mazumdar, ''Mitigating content poisoning in content centric network: A lightweight approach,'' in *Proc. 10th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2019, pp. 1–6, doi: 10.1109/ICCCNT45670.2019.8944392.

[116] G. Bianchi, A. Detti, A. Caponi, and N. B. Melazzi, ''Check before storing: What is the performance price of content integrity verification in LRU caching?'' *ACM SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 3, pp. 59–67, Jul. 2013, doi: 10.1145/2500098.2500106.

[117] A. Detti, A. Caponi, G. Tropea, G. Bianchi, and N. Blefari-Melazzi, ''On the interplay among naming, content validity and caching in information centric networks,'' in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 2108–2113, doi: 10.1109/GLOCOM.2013.6831386.

[118] C. Ghali, G. Tsudik, and E. Uzun, ''Needle in a haystack: Mitigating content poisoning in named-data networking,'' in *Proc. Workshop Secur. Emerg. Netw. Technol.* San Diego, CA, USA: Internet Society, 2014, pp. 1–10. [Online]. Available: https://www.ndss-symposium.org/ndss2014/workshop-security-emerging-networking-technologies-sent-2014-programme/needle-haystack-mitigating-content-poisoning-named-data-networking, doi: 10.14722/sent.2014.23014.

[119] A. Afanasyev, C. Yi, L. Wang, B. Zhang, and L. Zhang, ''Map-and-encap for scaling NDN routing,'' UCLA, NDN, Tech. Rep. NDN-0004, 2015, p. 6. [Online]. Available: http://named-data.net/techreports.html

[120] M. Bari, S. Chowdhury, R. Ahmed, R. Boutaba, and B. Mathieu, ''A survey of naming and routing in information-centric networks,'' *IEEE Commun. Mag.*, vol. 50, no. 12, pp. 44–53, Dec. 2012. [Online]. Available: http://ieeexplore.ieee.org/document/6384450/, doi: 10.1109/MCOM.2012.6384450.

[121] A. Afanasyev, C. Yi, L. Wang, B. Zhang, and L. Zhang, ''Scaling NDN routing: Old tale, new design,'' NDN Project, Tech. Rep. NDN-0004, 2013. [Online]. Available: https://named-data.net/publications/techreports/ndn-tr-4-scalingndn-routing/

[122] H. Kang, Y. Zhu, Y. Tao, and J. Yang, ''An in-network collaborative verification mechanism for defending content poisoning in named data networking,'' in *Proc. 1st IEEE Int. Conf. Hot Inf.-Centric Netw. (HotICN)*, Aug. 2018, pp. 46–50, doi: 10.1109/HOTICN.2018.8606003.

[123] S. Adithya, G. G. Karthik, H. Hariharan, and V. Vetriselvi, ''Assuaging cache based attacks in named data network,'' in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Mar. 2016, pp. 872–876, doi: 10.1109/WiSPNET.2016.7566256.

[124] C. Yi, A. Afanasyev, I. Moiseenko, L. Wang, B. Zhang, and L. Zhang, ''A case for stateful forwarding plane,'' *Comput. Commun.*, vol. 36, no. 7, pp. 779–791, Apr. 2013. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0140366413000236, doi: 10.1016/j.comcom.2013.01.005.

[125] S. DiBenedetto and C. Papadopoulos, ''Mitigating poisoned content with forwarding strategy,'' in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2016, pp. 164–169, doi: 10.1109/INFCOMW.2016.7562065.

[126] W. Cui, Y. Li, Y. Xin, and C. Liu, ''Feedback-based content poisoning mitigation in named data networking,'' in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2018, pp. 759–765, doi: 10.1109/ISCC.2018.8538609.

[127] W. Cui, Y. Li, Y. Zhang, C. Liu, and M. Zhan, ''An ant colony algorithm based content poisoning mitigation in named data networking,'' in *Proc. 18th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./13th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2019, pp. 176–183, doi: 10.1109/TrustCom/BigDataSE.2019.00032.

[128] D. Wu, Z. Xu, B. Chen, and Y. Zhang, ''What if routers are malicious? Mitigating content poisoning attack in NDN,'' in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2016, pp. 481–488, doi: 10.1109/TrustCom.2016.0100.

[129] I. A. Kapetanidou, C.-A. Sarros, and V. Tsaoussidis, ''Reputation-based trust approaches in named data networking,'' *Future Internet*, vol. 11, no. 11, p. 241, Nov. 2019. [Online]. Available: https://www.mdpi.com/1999-5903/11/11/241, doi: 10.3390/fi11110241.

[130] Z. Rezaeifar, J. Wang, and H. Oh, ''A trust-based method for mitigating cache poisoning in name data networking,'' *J. Netw. Comput. Appl.*, vol. 104, pp. 117–132, Feb. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804517304046, doi: 10.1016/j.jnca.2017.12.013.

[131] H. L. Mai, M. Aouadj, G. Doyen, D. Kondo, X. Marchal, T. Cholez, E. M. de Oca, and W. Mallouli, "Implementation of content poisoning attack detection and reaction in virtualized NDN networks," in *Proc. 21st Conf. Innov. Clouds, Internet Netw. Workshops (ICIN)*, Feb. 2018, pp. 1–3, doi: 10.1109/ICIN.2018.8401591.

[132] T. Nguyen, H.-L. Mai, G. Doyen, R. Cogranne, W. Mallouli, E. M. D. Oca, and O. Festor, "A security monitoring plane for named data networking deployment," *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 88–94, Nov. 2018, doi: 10.1109/MCOM.2018.1701135.

[133] I. A. Kapetanidou, S. Malagaris, and V. Tsaoussidis, "Avoiding notorious content sources: A content-poisoning attack mitigation approach," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2022, pp. 1–6, doi: 10.1109/ISCC55528.2022.9912936.

[134] E. Dogruluk, A. Costa, and J. Macedo, "Evaluating privacy attacks in named data network," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Messina, Italy, Jun. 2016, pp. 1251–1256. [Online]. Available: http://ieeexplore.ieee.org/document/7543908/, doi: 10.1109/ISCC.2016.7543908.

[135] A. Djama, B. Djamaa, and M. R. Senouci, "TCP/IP and ICN networking technologies for the Internet of Things: A comparative study," in *Proc. Int. Conf. Netw. Adv. Syst. (ICNAS)*, Annaba, Algeria, Jun. 2019, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/8807890/, doi: 10.1109/ICNAS.2019.8807890.

[136] H. Khelifi, S. Luo, B. Nour, and S. C. Shah, "Security and privacy issues in vehicular named data networks: An overview," *Mobile Inf. Syst.*, vol. 2018, pp. 1–11, Sep. 2018. [Online]. Available: https://www.hindawi.com/journals/misy/2018/5672154/, doi: 10.1155/2018/5672154.

MOHAMMAD SHAHRUL MOHD SHAH received the B.C.S. degree in network engineering and the M.C.S. degree in software development from Universiti Malaysia Sabah, Malaysia, in 2017 and 2019, respectively, where he is currently pursuing the Ph.D. degree in computer science with the Faculty of Computing and Informatics. In 2019, he joined as a Research Assistant with the Faculty of Computing and Informatics, Universiti Malaysia Sabah. His current research interests include named data networking, the Internet of Things, and networking.

YU-BENG LEAU (Senior Member, IEEE) received the B.Sc. degree in multimedia technology from Universiti Malaysia Sabah, the M.Sc. degree in information security degree from Universiti Teknologi Malaysia, and the Ph.D. degree in internet infrastructures security from University Sains Malaysia.

He is currently a Senior Lecturer of computer science with the Faculty of Computing and Informatics, Universiti Malaysia Sabah. His current research interests include intrusion detection and prediction, network security situation awareness, IPv6 security, the Internet of Things (IoT), and information centric networks (ICN).

MOHAMMED ANBAR (Member, IEEE) received the bachelor's degree in computer system engineering from Al-Azhar University, Palestine, the M.Sc. degree in information technology from Universiti Utara Malaysia (UUM), Malaysia, and the Ph.D. degree in advanced internet security and monitoring from University Sains Malaysia (USM).

He is currently a Senior Lecturer with the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His research interests include malware detection, web security, intrusion detection systems (IDS), intrusion prevention systems (IPS), network monitoring, the Internet of Things (IoT), and IPv6 security.

ALI ABDULQADER BIN-SALEM received the B.S. degree in computer science from Al-Ahgaff University, Yemen, in 2006, the M.S. degree in computer science from Universiti Sains Malaysia (USM), Malaysia, in 2009, and the Ph.D. degree from National Advanced IPv6 Center (NAv6), USM, in 2017.

He was involved as a System Operator in the East Asia-wide AI3 [Ay-triple-Ei] (Asian Internet Interconnections Initiative) Project, to help the use of Unidirectional Links over Satellite for interactive multimedia communications. He has been a Reviewer in many journals, including *Wireless Personal Communications*, *Journal of Internet Technology*, and *Mobile Information Systems*, and conferences, including the Second and Third International Conference on Advances in Cybersecurity (ACeS). His current research interests include the IoT, wireless LAN, QoS, 4G/5G/6G networks, cross-layer, optimization techniques, machine learning, distributed systems, and client-server architecture.