Hierarchical Naming Scheme in Named Data Networking for Internet of Things: A Review and Future Security Challenges

MOHAMMAD SHAHRUL MOHD SHAH¹, YU-BENG LEAU¹, (Senior Member, IEEE), ZHIWEI YAN², AND MOHAMMED ANBAR³, (Member, IEEE)

¹Faculty of Computing and Informatics, Universiti Malaysia Sabah, Kota Kinabalu 88400, Malaysia
²China Internet Network of Information Center, Beijing 100083, China
³National Advanced IPv6 Centre, Universiti Sains Malaysia, Gelugor 11700, Malaysia

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

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

ABSTRACT The proliferation of connected devices in the Internet of Things (IoT) presents a connectivity challenge. The future internet will require a paradigm shift in which content is evaluated on the basis of “What” it is rather than “Where” it originated. ICN’s goal is to provide the benefits of name-based content addressing in order to facilitate scalable content distribution, security, mobility, and trust. NDN is a new internet architecture that evolved from Content-Centric Networking (CCN). NDN is viewed as a solution to the IoT’s challenges, as well as a way to transcend the IP paradigm. With IoT systems that had a number of challenging characteristics to satisfy, including heterogeneous devices, resource constraints, and energy efficiency. Due to the fact that NDN native features deliver data via hierarchically structured names, it offer promising solutions for current research integrating NDN into IoT. The review discusses the significance of naming, its influence, and security factor. Additionally, research challenges in the areas of naming and security will be discussed. The primary objective of this review is to give a new facelift to a new integrating naming convention for NDN.

INDEX TERMS Internet of Things, information-centric networking, named data networking, hierarchical naming scheme, NDN-IoT security, future internet.

I. INTRODUCTION

The goal of the Internet of Things (IoT) [1] is to connect heterogeneous devices to the Internet in order to facilitate data sharing. The terms “Internet of Things” network was first coined in 1999 by British scientist “Kevin Ashton”, He attributed it into a massive deployment of interconnected network of devices (things) connected with radio frequency identification (RFID), technology [2]. With growing number of interconnected objects, the growth shown that by 2025 there will be 75 Billion connected objects to the Internet [3].

Given the staggering number of objects connected to the current Internet, adopting a unique IP address raises the stakes network will have to deal with. The traditional internet architecture, which is host-centric based, will create a platform that will allow a devices to stay connected in order to exchange and retrieve desired content via the network. IoT networking is primarily based on the TCP/IP protocol stack, which was originally designed to meet the needs of wired network in interconnecting computers, printers, or any other active equipment without regard for resource limitations. Consequently, TCP/IP as a host-centric communication protocol cannot meet the ever-increasing IoT requirements. Information Centric Networking [4] has been designated as the future internet to fulfill thesee demands, due to native features that supports IoT. In ICN, three main terminology is used [5]: Named Data Objects (NDO), publisher, and requestor. Content in ICN is uniquely identified by location-independent names, with the goal of efficient NDO dissemination and retrieval on 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 alligned with ICN goals to provide users with better perspective of what could have been accomplished compared to current Internet architecture.

Furthermore, Named Data Networking (NDN) [6] is one of the ICN instances and approaches with the purpose of centering communication processes around the role of content such that retrieving processes may well be completed more efficiently 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 [7], [8]. The rest of this paper is organized as follows: Section II will provide an overview of NDN in terms of naming, security, and application in the context of IoT. Section III discussed existing naming and security in IoT. Section IV discusses the current challenges. Finally, section V concludes the paper.

A. RELATED WORK

There have been a variety of surveys on ICN and NDN, with an emphasis on ICN as a general architecture [9]–[11]. Some surveys give an insight on features like caching [12], mobility [10], [13], routing and forwarding [14], [15]. The deployment of IoT in ICN has become more common, and number of research has grown due to suitability that ICN hold.

The importance of naming and security in NDN-IoT cannot be overstated. This survey was conducted to determine how significant they are in the context of the IoT. There have been a few of studies that have tried to classify and categorise the way people name things, like in [16], where authors group ICN instances into their naming structure such as PSIRP/PURSUIT, DONA [17], MobilityFirst, NDN, and CONVERGENCE are ICN instances into flat, hierarchical, and hybrid naming scheme categories. Author breaks down the challenges into five categories: congestion control, security, availability, erratic behaviour, and multi-source multi-destination. The author categorises the approaches to naming schemes based on their usability in scenarios such as user-centric environments, object-centric environments, cloud computing, and software defined networking. However, this survey falls short in terms of including naming in the IoT application use-case and naming in ICN as a whole without the IoT context. The same can be said for the paper in [18], which focuses on naming, name resolution, and data routing for ICN instances such as DONA [17], NetInf [19], [20], and Pursuit. Authors who specialize in flat naming scheme without the IoT use-case application.

Then, we move towards the use of naming in IoT applications use-case, the first ICN-IoT surveys is in [21], first paper raises a questions the abilities of NDN-IoT by discussed technical challenges, deployment options and benefits from reaping NDN in IoT. Additional work from the author is in [22], suggesting a guidelines and provides challenges and opportunities in integrating IoT with ICN, without taking and evaluating all of the research available in integration of ICN-IoT.

Another survey is in [23], provides a more detailed use case of NDN in IoT. The detailed review focuses on NDN and its architecture and major features embedded in ICN architecture such as device and data naming, caching, access controls, forwarding, data aggregation, and device configuration. The naming section is insufficiently detailed for readers to dive in and learn more about the naming conventions that the NDN revolves around. The authors conduct a comparative analysis of the collected works, gathering the characteristics supported by each solution. Despite this, a few key features, such as security, quality of service, and mobility support, were overlooked.

In [19], authors presented the main concepts of NDN in the IoT infrastructure, including naming, routing, forwarding, and caching. Authors highlighted the proper design choices for NDN in IoT, such as NDN packet length, caching, data aggregation in wireless networks, naming problems in wireless networks, and routing scalability in NDN. Nonetheless, in terms of discussed reviewed literature, surveyed article falls short in naming resolution scheme. Our survey focused on hierarchical naming with an emphasis on NDN for IoT in the best way possible.

B. CONTRIBUTIONS

This review paper discusses regarding NDN’s hierarchical naming, with a focus on how it fits with IoT applications: namely, NDN-IoT. As part of our work, we want to make the NDN-IoT naming system more explicit about the security issues that will arise. Which are based on the trust model used in the IoT application. The following are the paper’s main contributions:

1) This article compiles the NDN-IoT naming scheme, with a particular emphasis on Hierarchical and Hybrid naming schemes.
2) Based on their security concerns, the paper constructs a hierarchical naming scheme and a hybrid naming strategy in IoT environment.
3) The paper discusses the challenges inherent in designing and selecting an appropriate naming scheme in order to increase its security.

Our paper focuses on the security implications of the NDN naming in IoT applications. There are a few more obstacles to overcome in terms of research, in deciding which naming scheme is the most secure and suited best for IoT.

II. NAMED DATA NETWORKING

Previously, we discovered that NDN architecture has emerged as an entirely different design that may be used in the context of the IoT ecosystem. Naming and NDN are complementary; learning more about the architecture of NDN will reveals its potential.

A. BACKGROUND OF NDN

Named Data Networking (NDN) comes from its predecessor Content Centric Networking (CCN) [24], was one of the
The design of the NDN protocol is as follows [28]: Data Object (NDO) [27] is one of ICN’s core characteristics. Before the architecture and execution of NDN, the Named and name structure of application development must all come from domain names, which is still in a dispute. The name-detection challenge in naming is to resolve the name for the top-level domain names that allow for name aggregation should be utilised. There are four major naming types in ICN:

1) **Hierarchical naming schemes**: A Naming scheme that composed of a set of human-readable components, user-friendly, bring semantic meaning to users and hierarchically structured naming scheme; similar to URL hierarchical semantic that hold “/” (separator) in between components of the name. The Hierarchical naming scheme helps network scalability and stability due to the name prefix’s ability to be aggregated.

2) **Flat naming schemes**: A naming scheme that produced from cryptographic hashing of the content. It varies from hierarchical naming in both semantic meanings, where flat naming is not hierarchically structured and is not human readable. Flat naming cannot enhance scalability, as it did not have support for aggregation resulting in an outburst in the size of the routing and forwarding table.

3) **Attribute-based naming scheme**: A naming scheme that composed of content attributes (name, types, and set of possible values). It allows different kinds of information reside inside the names. The names could be an indifferent form like plain text, encoded, encrypted, and machine-readable.

4) **Hybrid-based naming scheme**: A naming scheme that combines two or three from the above-mentioned naming schemes. The main idea is to combines the best aspects of each naming scheme in improving scalability, efficiency, and security. Each naming has its own strength, such as hierarchical naming: provide name aggregation to improve lookup time, flat naming in which its ability to have fixed length name to save memory consumption and attribute naming in ease of searching for keyword process.

Hierarchical and hybrid naming are widely deployed in IoT use-case, this is due to ease of structuring the name in form of hierarchy. Not only that, NDN native features that requires all content objects to be signed would help in securing IoT objects in the network.

C. **NDN IN THE CONTEXT OF IoT**

With IoT goals to form large network of interconnected devices and the ability to gather data while providing a wider range of benefits [20]. Devices are bound to resource constrained, mobility factor, and traffic patterns raise a challenges. With this, due to the requirements of IoT satisfies by the intrinsic features of NDN, the suitability of using NDN as an IoT communication model appears to be a potential solution as shown in Table 1. IP-based communication options likewise meet the primary IoT criteria, but the distinction between “host-centric” and “content-centric”
TABLE 1. IoT requirements and native NDN support.

| IoT Requirements | NDN Features |
|------------------|--------------|
| Naming           | Natively supported by hierarchical naming mechanism |
| Scalability      | Need additional mechanism to work and it is supported by naming, caching, anycast/multicast mechanism. |
| Security         | Supported by securing the packet mechanism. |
| Lightweight design | Supported with the ability of multicast/anycast and caching ability. |
| Mobility         | Consumer mobility: Supported. Producer mobility: Needs additional mechanism |
| Caching          | Supported at the layer 3 (network layer) |

...continued from previous text...

communication approaches remains the most compelling justification for their applicability in the context of IoT. IoT main characteristics consist of five parts:

- **Devices**: Devices in IoT networks composed of sensors and actuators.
- **Connectivity**: Cloud-based or machine-to-machine.
- **Actions**: Decisions that are automatic
- **Intelligence**: Ability to analyse.
- **Communication**: Consist of content-retrieval and publish-subscribe.

The requirements that the IoT has fit well with what ICN brings to the table as a solution for future internet architecture [11], which is why NDN is best suited for IoT. Despite the fact that ICN is still in a growing phase, there are still challenges need to be addressed. Since IoT relies on the content, and ICN with its content-centric characteristic; it appears like the integrating process between them is realistic. Since communication standards occur in IoT performed in a various of applications, the standard chosen must take into account on how networks and applications will be affected. These standards include Bluetooth, Radio Frequency Identification (RFID), Wireless Fidelity (Wi-Fi), Ziqbee, Sigfox.

Authors in [29], investigate the relationship between the internet of things and both TCP/IP and ICN, as well as a comparison study. The benefits and drawbacks of these architectures are demonstrated to determine which are best suited for IoT. According to the comparison, each architecture satisfies the main needs of IoT requirements. However, TCP/IP needs to be redesigned so that it able to satisfy IoT requirements such as resources constraints and mobility where ICN natively able to do. NDN’s intrinsic features as shown in Table 1 are capable of solving multiple IoT requirements:

- **Naming**: With NDN native hierarchical naming structure, it can help in efficiently extract and manage data from the IoT ecosystem. Heterogeneous devices can be connected using these characteristics if the semantic meanings of the content names for network and application-specific design allow it. The content name in NDN can be modified to match a variety of devices and applications use case.
- **Scalability**: IoT presents a major scalability issue, particularly when combined with the incoming and continuous stream of information/content generated by huge number of devices. By giving IoT content a name, allowing it to be organised, and allowing users to expressly request the content they need rather than manually searching for it in a specific node. As a result, NDN-based IoT will have the potential to address these issues.
- **Security**: With various of IoT application use cases, the main idea behind IoT is to connect devices and sharing of data. With that, the need to protect the data from an attacker is one of the requirements to protect user privacy and data integrity. NDN modifies the network protocol’s thin waist and extends security support to the network layer, thereby lowering security concerns. The initial NDN method to secure the packet was to encrypt and secured the content rather than the communication channel by having the producer sign the data packet with his or her key before sending it across the network. The data packet’s signature ensures that the data’s integrity and authentication are not compromised.
- **Lightweight design**: In IoT environment, there are limitations and constraints bound factor needed to form an IoT ecosystem such as memory, storage, energy, and bandwidth. Memory, storage, energy, and bandwidth are only some of the capabilities of the nodes that make up the IoT ecosystem. For such a requirement, a lightweight design can be used to preserve network resources. The Internet Engineering Task Force (IETF) has developed recommendations [30] to assist developers in creating devices for limited environments.
- **Mobility**: Mobility support is one of the requirements in IoT, due to the physical size of the devices connected or sensors that is compact and frequently moved by users can help deployment in mobility oriented like smart vehicles to operate. With NDN location-independent support features, data can be requested by its name even users move from one location to another.

NDN architecture offers several valuable characteristics that makes it an excellent solution for IoT. Not only that, according to the authors in [31], they conducted a qualitative comparison assessment of most of ICN architecture such as DONA, PURSUIT, COMET, NetInf, CONVERGENCE, MobilityFirst and NDN, as a result they discovered that NDN is the best ICN solutions for IoT. The fact that NDN concepts align with the expectations of the IoT, there are several issues that need to be addressed such as naming and security aspect, will be discussed further in section III.

III. NAMING AND SECURITY IN NDN-IOT

A. NAMING SCHEME

1) HIERARCHICAL NAMING SCHEME

Named Data Networking employs a hierarchical structure intrinsically; semantics are not assigned to its name. Author in [32] visualize that service layer in ICN as contextualized information-centric bus (CIBUS), where it can serve different applications in IoT over which diverse set of service
producers and consumer that are co-exists. Then, In [33], author show how this concept can be applied to a home network and present a case of homenet based on CCN architecture with a focus on naming and service configuration. Current homenet proposed by the Internet Engineering Task Force (IETF) built on IPv6, which inherits fundamental IP problems such as security, mobility, and multicasting. With that, authors compared IPv6 proposal with ICN approach form in terms of service, control, complexity, and data plan features. Proposed architecture utilized hierarchical naming to leverage efficient content dissemination. The naming hierarchy consists of six levels:

1) **Access scope**: Identifies homenet instance and reachability scope of a service.
2) **Service scope**: Identifies type of service type such as security, climate-control and entertainment.
3) **Device scope**: Identifies the devices offering the service type.
4) **Content scope**: Identifies the types of content supplied to the devices.
5) **Access scope**: Policies: Identifies policies that needed to be follows for the consumer such as access control policies.
6) **Service API**: Identify the attributes that used in interacting with the service.

The high cost of ownership, inflexibility, and difficulties in providing security are all highlighted as challenges in implementing a home network. Content distribution and mobility can be assisted by a naming scheme and in-network caching capability. When compared to an IPv6-based home network, ICN has a reduced traffic overhead.

The authors in [34], proposed on creating an efficient platform enabling services in smart city environment using NDN architecture. Service provisioning are performed in three consecutive phases: discovery phase, security initialization phase and service usage phase. In discovery phase, subscriber discover remote publishers that can satisfy user requests. Then, in security initialization, user retrieves security information needed to access the packet. In final phase, service usage phase is where it can overlap with discovery phase due to user already get the content needed during the discovering of the publisher. Smart cities design contains a name space to classify and map all the services in ordered and hierarchical manner, to simplify routing operations. The drawbacks of proposed solution is with the implementation of hierarchical naming structure are long and name lookup process will be much longer.

Authors in [35] proposed privacy preserving in E- Health use-cases over NDN architecture, adapting an existing privacy attempt for NDN, named ANDiNA [36]. Proposed naming scheme comes from idea in [34], author retains human-readable structure defined by NDN and composed of four parts delimited by character “/”: /domain/IoT-service/service-specification/type-of-request/ optional-info. The first part is Iot-service, used to specifies routing information. Then, service-specification part, explicit type of transmitted data. The type-of request pat, specify priority of transmitted data. Lastly, the optional-info is based on unbounded NDN namespace in allowing integration of specific data. Author performed a comparison of their proposed scheme to IP-based solutions in [37], with the overhead evaluation result that indicates IP-based outperforms NDN. However, there is still factors need to be considered that include NDN is deployed as an overlay compared to an IP that suffer from high overhead.

After that, hierarchical naming has been applied in lighting automation control [38]. Providing a communication platform that is secure and efficient in order to achieve low latency that is sufficient for the lighting component to function. In total, three elements to the suggested namespace; (1) fixture-namepace, being used in routing operation, (2) /command, and (3) /randomizer /auth-tag.

The author in [39], proposed data-centric architecture design based on NDN deployed in Building Automation and Management Systems (BASs and BMSs), called NDN-BMS. In their proposed system, authors utilize hierarchical naming scheme because of its abilities in mapping to application-specific structure in the data thus simplify the complex distributed applications. Namespace structure of NDN-BMS start with root node prefix that represent common prefix fo UCLA campus (/ndn/ucla.edu/bms), then, two sub-namespaces /building for publishing data and /user for identity management shown in Fig.2(a)(b). In Fig.2(a), used for name of a sensor in data packet and indicates physical location of the sensor where panel j located inside studio 1 (hall/studio/1/data/panel/J), then (/voltage) indicates type of data, (/timestamp) indicates time of data received. While, in Fig.2(b), used for NDN-BMS able to uniquely identify its users, (/<key-id>) indicates to SHA256 digest of the public key that distinguishes numerous public keys belonging to the same user.

Authors in [40] proposed CCN based IoT named PHINet, deployed in Health-IoT applications. Due to IP-based deployment comes with an issues of scalability and host-centric nature, CCN/NDN provides better support that allows multicasting and mobility thus suited well for PHINet application. PHINet uses hierarchical naming in an NDN-based system by providing an ad-hoc platform where the application service can be implemented. Namespace shown in Table 3, (i.e./domain/userID/sensorID/timestring/processID).
Hierarchical naming framework for smart home proposed by [41], namely: NDOMUS (sMart home aUtomation Sys-
tems). Proposed framework is based on author previous work [21] that addresses high-level NDN architecture to be revised so it fit the IoT challenges. There are three main features in NDOMUS: naming scheme, service model and strategy for multi-party communications. In naming scheme, as shown in Table 4, there are two sub-namespace classes, namely: configuration and management and task namespace. Configuration and management namespace is used for home network initialization and stand by the prefix (/conf), same as in [38], where configuration and authorization manager register end devices assign to namespace which they operate and security details information. Proposed naming scheme support task aggregation to reduce number of request hence reduce number of network bandwidth. However, proposed scheme did not provide simulations on experiment and did not ensure security factor for transmitted information.

NDN hierarchical naming is implemented in a variety of use case, and in [42], naming being employed for underwater monitoring to collect information instead of using the traditional IP address. Naming schemes in NDN-IoT can be utilized in wide range of applications, the authors [43] proposed using NDN hybrid naming scheme in Intravehicular Communication (IVC) scenario. Two naming schemes included in the proposed method are device-based for differentiate numerous devices and location-based naming to ensure scalability in vehicular scenario designed to be hierarchical.

Introducing a Lightweight Named Object (LNO) [44] solution that stands for physical IoT objects. The solutions from LNO can be beneficial in programming simplicity, extended functionalities in the devices. Solutions that are presented will be using NDN hierarchical names to representing the IoT objects in the namespace shown in Table 2. Even the main functionality is lightweight, the names stretch into a few name structures as shown in a Table 2. To have mobility in IoT networks, this topological type naming is not advisable because of the connection in the devices constantly changing.

2) HYBRID NAMING SCHEME
In order to unleash the best features in naming scheme, ICN based hybrid naming scheme for IoT [9], integrates two or three naming schemes to provide them with a single framework to cooperate. The combination of the best features can improve data secrecy, network scalability and performance.

Authors in [45], proposed the NDN-HNS (Hybrid Naming Scheme) for IoT-based smart campuses. In their proposed naming scheme, the authors incorporate both hierarchical and flat structures, whilst still supporting both push and pull communication models. It has been used in “smart campus” use case because of its flexibility and ability to scale services by adding more devices, enabling them to become even smarter. The NDN-HNS naming scheme is made up of three unified name schemes: hierarchical, flat, and attributes. The authors recommended four naming processes, which are illustrated in Fig.3; the first part is the IoT application or Primary Root Prefix, which denotes the IoT application use case (for example, Smart Agriculture (SA), Smart E-Health (SHE), and Smart Transportation (ST)). Hierarchical components, also known as secondary root prefix, is the second type of component; contains the campus name, location, content originator or public key, and content type, as well as name management and aggregation in a hierarchical order. The third part is attribute components, which describes the content’s specifics. Lastly, the flat component, which secures the content by collecting the hashed value of either the content originator, content type, or content-sub type. The length of the name will be taken into account while determining scalability and speed of name lookup.

The advantages of hierarchical naming is to provide name aggregation which can serve each functionality, but having multiple hierarchical names like in [43] required to maintain a complex routing per state application. With that, rather than using multiple hierarchical names, author in [46] propose hybrid naming scheme that combines hierarchical names with keyword-based system to define IoT data in the network. Proposed scheme inspired by TagNet [47], modified version of Tagnet used of tag-based routing for local IoT domain. The proposed naming scheme composed of three
B. NDN-IoT SECURITY

The importance of security in any kind of networking communication cannot be overstated. In NDN, protocol design principles focus to have security as a property of data packets [50]. Addressing the security issues in NDN has been accomplished in a variety of ways, when compared to IP network security, NDN does not use the host model, hence it focuses on securing the content rather than the communication channel and implements content-based security [51]. A survey has been implemented in security, privacy and access control [52]. The security features that was surveyed was not in the context of IoT. In [53], [54], writers analyzed security attacks that NDN vulnerable to, such as interest flooding, cache privacy, cache pollution and content poisoning attack. Recent work has been implemented with ICN security issues and attacks when deployed into a wireless environment [55]. There are solutions for managing security in NDN for IoT:

1) ACCESS CONTROL

Digital Signatures is used to authenticate the content in NDN, encryption is performed if the content is private. NDN authenticates decoupling names and the content; data packets contain a signature over the name. The process of signed bindings is to establish and certify the content. Content-based security in NDN enables each of the data to become a self-authentication unit, to protect and implement a trust at the packet level. As for that, security can be applied to content-centric based is access control. A trusted server does not have to invoke access control policies, due to the private content can be decrypted only by the authorized user. NDN extensive survey has been implemented in [56] on access control in NDN that categorize the approach into two; Encryption-based and Encryption-independent and each one has its subclasses. But the surveyed limit to generic access control in NDN, not in the context of NDN for IoT.

The hierarchical naming scheme given in the use case of lighting control in the NDN is secured by application-specific access control [38]. In the proposed design, hierarchical naming is applied to provide a security element by combining a trust model with key attributes and access control. Both interests and data packets are natively supported by NDN security in terms of maintaining integrity and packet authentication. Generally, data packets are signed by their originator producers, however, signed interest is performed on the consumer side to verify that actions are requested only approved authenticated entities. The design choices used in the lighting control use-case are motivated by the need for efficiency and the preservation for privacy. In accordance with the naming strategy, tags are used to indicate an output of an authenticated interest in the form of either public key or symmetric authentication, based on the location. There are four parties involved in the development framework are the Authentication Manager (AM) to manage network’s PKI and authorized communication by using share symmetric keys; the Configuration Manager (CM) to assigns fixtures to NDN namespace; the Fixtures (Fix) to receive authenticated command in form of private key and verify the received command to be return in form of signed content if the successfully verified. With the use of hierarchical NDN naming that restricts access to fixtures to provide security, long hierarchical names still a challenge for a lookup process. Not only that, using RSA and HMAC increase the complexity of processing.

In hierarchical naming of NDN-BMS [39], authors provide access control mechanism that is deployed at University of California at Los Angeles (UCLA). Proposed access control scheme different from [38], where here, author target that
data collection process performed in situations where low-latency and direct communication is not needed. NDN-based utilized identity-based access control scheme where Access Control List is configured at each gateway to identify user that has been granted access by checking user Access Privilege List (APL). As BMS initially proposed in [25], having multiple namespace that separates it from trust model. In [39], proposed scheme have two namespaces used: data access for physical building applications and trust management for key identifier. NDN-BMS encrypts sensor data with a shared symmetric key and distributes the shared symmetric key using an asymmetric encryption algorithm.

While, security proposed in [33] is to perform private information and access restricted access to the information. A hierarchical naming scheme in homenet meets the naming requirement required to secure the naming scheme. As in III, the hierarchical naming proposed level contained six levels and the security aspect is at level 3 of the hierarchy. The hierarchical naming helps to express the policy enforcement.

The author in [41] proposed an access control for hierarchical naming and provides a namespace specific to its task. The concept of relying on sensitive information is the same as in [38] which the information requires authentication, privacy and integrity. As shown in Table 4, naming namespace, the framework proposed using configuration manager in the NDN namespace to hold unique key pair. After that, the authorization manager can determine whether access should be given to the application and maintain the full access control for an application. There have been no implementation results to be reported.

Authors [57] proposed a lightweight access control for the constrained environment over NDN (NDN-ACE). It employs hierarchical naming in NDN to express access control policies to command senders and authorized access to the services they are intended to access. Naming used in NDN-ACE used to express services, identities and access control as a sequence number. Privacy aspect in NDN-ACE naming is considered as a major concern due to names being exposed to an attacker. Authorization and authentication are managed by an authorization server (AS) to perform access control.

Author in [58] proposed to design a middleware to address security and privacy in ICN-IoT. Author aims to develop effective access control system and provide trust model that suited to handles the communication between entities and relationships. There are five components involved: embedded systems, aggregator, Local Service Gateway (LSG), ICN-IoT Server and services. In embedded systems, sensors serve a function to transmit data to aggregator. While, gateway serve as local gateway to bridge the communication. In LSG, connect local and global IoT system to enforces data access policies for local IoT devices. In ICN-IoT server, manage lookup services. Last component is services, act as application interfaces used to interact with ICN-IoT server. Interaction of these entities integrated to security solutions: device discovery, service discovery, user registration and content delivery. However, there is no evaluation of the proposed mechanism included.

Edge re-encryption-based Access Control (ERE-AC) proposed in [59], encryption of the content in NDN using the symmetric key and the content key will go through two times of encryption process at the producer and edge router. Simulation results indicate ERE-AC effectively controls the delay compared to the Encryption-based Access Control Model (EPB-ACM). The author’s vision is to implement access control in solving cache privacy challenges in NDN.

2) CONTENT SECURITY
Content security is one of the key important and fundamental criteria in data centric networking [7]. Furthermore, the demand for network and content security has risen due to number of heterogeneous devices connected in the Internet of Things. Authors in [60], utilizing hybrid naming to secured the content using flat section of proposed naming scheme and presented it in Base64 format. The hybrid naming scheme contributes significantly to security aspect by including the hash characteristics in the final section of the name. The hybrid naming scheme contributes significantly to security aspect by including the hash characteristics in the final section of the name.

With the hybrid naming proposed in [45], [61], author take advantage of the flat component to solve the challenges of long hierarchical names. Author secured the device with FNV-1a hash, noncryptographic hashing algorithm. Various Internet of Things use-case applications have different security goals; for example, enhancing privacy is critical in the E-health IoT use case [35], [37]. This security solution is developed primarily on the enhancement and modification of ANDaNA and built on top of Identity-based Cryptography (IBC) primitives that are specifically tailored to the E-Health use-case. The initial step in communicating through ANDaNA is to generate an ephemeral circuit with two layers of encryption to provide anonymity [62]: then choose two anonymizing routers (ARs), namely entry (AR1) and exit (AR2) router. Generating an interest packet that is wrapped twice using public keys to fetch the desired data. Firstly, sent to AR1 for decryption of the first wrapped and generates new named interest, then sent to AR2 for final decryption so that it can be forward to producer so that data packet can be returned in reverse path and encrypted with symmetric keys.

Healthcare IoT industry require the abilities to solve challenges like managing the sensor and data [63]. Author in [64] proposed NDN-based smart healthcare IoT system (SmartHealth-NDNoT). The use-case is to provide remote monitoring at a low cost. Not only that, the proposed system function is to collect, transfer and analyze patient’s personal health data by using NDN naming convention. Proposed architecture that support static and dynamic content are composed of four layers: embedded systems, gateway, database, and central controller. In embedded system, is where different kind of sensors can monitor patient health and gather data
at real-time. In gateway layer, data collected being send to service centres. While in central controller, data collected being analyses. In last layer, where routing and forwarding updates are performed. Author then further their research in healthcare IoT industry by proposing platform for smart healthcare: NHealthIoT [65]. Author uses pure-NDN-Based machine-to-machine communication for verification of content. From this, healthcare applications that require privacy and integrity of patients should considered trust management in system.

As IoT requirement are bounds to devices capability, complicated cryptographic algorithms can cause significant overhead. With the use of Elliptic Curve cryptography (ECC) in IoT [66], it considered to be more suitable for building lightweight public key crypto-system (PKC) with its advantage of small key size and low arithmetic requirements. As shown by author in [67], author proposed a scheme to prevent content poisoning attack in NDN-based IoT using lightweight Hyperelliptic curve algorithm. Author also proposed lightweight OnDemand verification authentication to mitigate content poisoning attack by allowing providers and client register themselves with network manager using their identities. After that, public and private keys are generated by their identities to retrieve content.

Maintaining the content integrity can be achieved to securing the content itself with the use of signed data packet before distributed to router, from NDN native nature symmetric and asymmetric encryption can be supported by using public key encryption and the use of private key decryption. Using other technology like integration encryption of blockchain also implemented. In [68], proposed hierarchical identity-based security mechanism by Blockchain (HISM-B) for NDN. Name of the data used to bind with the public key then embedded into the data packet to ensuring authentication and integrity of the data packet. Domains involved are information service entity (ISE) and Private Key Generator (PKG) used in providing security service. The ISE creates a blockchain network for managing public keys. Hierarchical naming is used to request the data packet. Then, the router will generate a key and parameter (PARAM) that includes the validation period and returned in the form of the data packet. The payload returned that containing PARAM and the validation period provide the secure service.

Employing Access control in IoT devices is still limited due to computation power, memory consumption. Each mechanism provided by access control have their benefits and varies from each use case. Communication semantics offer by NDN can benefit NDN based IoT due to the simpler stack to perform communication and the possibility to create an IoT framework.

**IV. DISCUSSIONS AND FUTURE WORK**

Content-based communication highly depends on naming because it affects routing, forwarding, caching, and the security of the information exchanged. Although NDN’s naming and security components are not mutually exclusive, it is possible to preserve the integrity of the content by incorporating the security methods into the name.

1) **NAMING**

In NDN networks, the naming scheme designed is the most important aspect in developing a naming scheme because it will affect other functionalities if prepared incorrectly. To create a naming scheme, particularly for NDN for IoT, some challenges such as name length, name aggregation, and complexity must be overcome.

- **Lengthiness of the names:** Namespaces and prefixes size must be considered; using long and unbounded names may result in high memory usage and a complex lookup process that will affecting scalability. In both naming approaches are unbounded in terms of name length; however, hierarchical naming has a slight advantage in scaling better than hybrid naming if it incorporates flat names; this is due to name prefixes and services shared throughout the forwarding data structure.

- **Name aggregation:** In contrast to IP addresses, the last part of the prefix must be matched throughout the lookup process, and it can be improved by using hierarchical structure that provides name aggregation. With this, achieving low latency and accuracy can be achieved.

- **Complexity:** With the usage of Application Program Interface (APIs), the degree of difficulty in adapting NDN to IoT has raised a complexity challenge. The designing step must include modifications in integrating software, hardware, and protocols must be made. In terms of implementation, testing, and cost; native hierarchical naming is less complicated than hybrid naming. It may be difficult to implement with dynamic IoT content due to the use of flat names that used hash techniques.

There is currently no clear consensus on whether hierarchical or hybrid naming schemes should be employed. Each naming scheme has a specific application. The hierarchical naming approach and hybrid naming that incorporates hierarchical naming are both human-readable. For future development, utilizing hierarchical naming makes it easier to aggregate, but its ability to scale has not been studied and need to find a solution for it. Suppose the deployment is on a large scale, in that case, the length of the content name should be considered because the lookup process in ICN forwarding data structure [69] can be increase before it affects content access latency, which is especially important in the data on demand use-case (e.g., military, healthcare, transportation). To meet these issues, additional research is still required to develop naming solutions that meet all of the identified constraints.

2) **SECURITY**

Security concept in NDN is different because of the data itself has built-in security features that protect it. When paired with the record originator, the name allows the origin of the data to be determined. As used in NDN, data-centric security provides for a great deal of flexibility in designing trust
models for consumers, publishers, and applications. With one of the requirements in IoT is to provide security services for its user, the deployment of security support at network layer in ICN can provide data authentication and content integrity be preserved. As we classified in Section III, there are two categories of security approaches: access control and content security. The challenges that we find are:

**Authentication:** With wide range of IoT applications, in most cases, there is a situation where applications require users to verify their credential; for an example, when we want to execute a task or action from a sensor/actuator, there are needs to allowed authorized entity only. As currently, security mechanism in ICN is only used to protect data packets and unsupported for request authentication.

**Complexity:** In IoT context, routers role have not been specify the task it performed. The decision of the use of cryptography or hash function rather than Public key Cryptography (PKI) will reduce its complexity. Key management and distribution is still an open challenges for IoT.

**Lightweight solution:** NDN approach that envisions access control in its application requires further research to make IoT devices suitable with limited processing power and memory. Future research in the NDN naming scheme for IoT in terms of security, includes preserving data confidentiality (read by others) and integrity (not been tempered with); for preserving data integrity and authenticity, message exchanged is digitally signed and binding process of certificates between content and its name will preserved the integrity of the data, for preserving data confidentiality, access control and encryption in caching process is needed.

**Versatility:** As ICN native data-centric features considered exclusive, generic security measure to suit wide range of IoT applications. Each application use case should consider their security goals that they are trying to achieve such as confidentiality, integrity, and non-repudiation.

The importance of security in network communication is the ability to ease of deployment in IoT use cases. NDN basic hierarchical naming, as opposed to the hybrid naming system, can secure the basic IoT use-case without adding new features or components. From section III, we can conclude that, benefits of hierarchical naming in NDN-IoT to provide access control instead of hybrid naming. The use case of any IoT application will define which naming system is used to secure the framework. Unencrypted content can cause lack of data confidentiality, and with encrypted content can utilize the benefits of caching in NDN. With this, due to numerous types of encryption technique (symmetric encryption, asymmetric encryption, elliptic curve encryption, etc); future work will help the security aspect by choosing the best suited method for NDN-IoT application. Furthermore, research should be focused more on utilizing Lightweight Elliptic cryptography (ECC) to make up a Public Key Cryptosystem.

Table 5 shows summary of all the ICN-IoT implementation in terms naming and security features, with advantages and disadvantages of past proposed scheme.

### Table 5. Summary of ICN in IoT naming and security.

| Ref      | Model             | IoT Applications | Naming scheme | Security Methodology | Simulators | Parameters Calculated | Advantages | Disadvantages |
|----------|-------------------|------------------|---------------|---------------------|------------|-----------------------|------------|---------------|
| [32], [33] | CCN               | Smart Home       | Hierarchical  | -                   | -          | -                     | (i) Can perform multi-consumers and multi-source      |
| [34]     | NDN               | Smart City       | Hierarchical  | -                   | -          | -                     | (i) Can leverage hierarchical naming in routing operations (ii) Long names causes large overhead |
| [35], [37] | NDN              | Smart Healthcare | Hierarchical  | Routing by modification of ANMNA and BIC symmetric encryption scheme | nSDIM      | 1. Transmission delay 2. Overhead evaluation | (i) NDN-based IoT deployment may simplify compared to IPv6-based (ii) Outperforms by IPv-based solution |
| [38]     | NDN               | Lighting Control | Hierarchical  | Access control Implicit into naming scheme | -          | -                     | (i) Security aspect embedded into naming scheme (ii) Long hierarchical name affect lookup process |
| [39]     | NDN               | Building Management System | Hierarchical | Access control Gateway to manage ACL symmetric key cryptograph | Provotiret with NDN-FS library | - | (i) Security approach made better compared to securing communication channel (ii) Resistant to DoS attacks (iii) Utilizing gateway can be complex and expensive |
| [42], [44] | NDN              | Smart Sense Network | Hierarchical  | -                   | -          | -                     | (i) Can perform multi-consumers and multi-source      |
| [44]     | NDN               | Smart Camera     | Hierarchical  | -                   | NFD v0.5.1 | Average number of required FIB entries per node | (i) Lightweight functionality (ii) Mobility factor will be restrained from proposed naming topology |
| [45]     | CCN               | Smart Campus     | Hierarchical and Flat naming | Secure device using 32-bit PN1 is noncryptographic hashing algorithm | CCNs-Cronki | 1. Satisfied Interest Rate 2. Average Latency 3. Transmission of Interest Packets 4. Number of Hops 5. Interest Aggregation | (i) Support static and mobile nodes (ii) Low latency aggregation with combination of names (iii) Forwarding packet delay when reaches node that cannot control retrieval time |
| [45], [46] | ICN               | Smart Building   | Hierarchical and Flat naming | - | - | 1. Bandwidth Efficiency 2. Lookup Performance | (i) Support Mobility (ii) Contains fine-grained (iii) Provides short lookup and routing process (iv) Content name is not homogenous |
| [54]     | ICN               | ICN-IoT Services | - | Secure device discovery, Secure service discovery, Secure caching service, Secure content delivery | XML diagram | - | (i) Secured content delivery (ii) No evaluation and implementation |
| [55]     | NDN               | Video Streaming  | - | Symmetric key encryption | nSDIM      | 1. The performance of bit rate 2. Content receiver delay | (i) Content producers need to always online (ii) Computational overhead |
| [60]     | ICN               | Volcanic Ashflow Network | Hierarchical and Flat naming | Basic4 format or content name | nSDIM      | - | (i) Lightweight (ii) Support low-powered devices (iii) Naming scheme too long (iv) Lack of query mechanism for data extraction |
V. CONCLUSION

This research aims to analyze and investigate the most important attacks with their proposed mitigation methods in NDN-IoT. To summarize, we believe that the primary challenges in NDN-IoT are ensuring data confidentiality and integrity in IoT applications. The importance of naming and security issues in relation to these security requirements is emphasized in this paper. In NDN, we focused on hierarchical names and security, particularly in the context of an Internet of Things application. The issues that arise and the difficulties that NDN faces have also been highlighted. Thus, this work can be expanded to include the selection of the appropriate naming scheme and encryption technique for securing the NDN-based IoT architecture. In the future, we intend to analyze the encryption countermeasures for securing the NDN-IoT, which can be quantified in terms of network performance, as well as the impact of the chosen naming scheme, encryption technique, and native digital signature on the NDN-IoT model’s security.

ACKNOWLEDGMENT

The authors would like to thank the Ministry of Higher Education Malaysia (MoHE), and Faculty of Computing and Informatics, Universiti Malaysia Sabah, and also would like to thank the anonymous reviewers, whose valuable comments and suggestions allowed to improve this work both in scope and presentation.

REFERENCES

[1] A. Rayes and S. Salam, Internet of Things From Hype to Reality: The Road to Digitization, 2nd ed. Cham, Switzerland: Springer, 2019. [Online]. Available: https://www.springer.com/gp/book/9783319995151

[2] K. Ashton, “That ‘Internet of Things’ thing,” RFID J., vol. 22, no. 7, pp. 97–114, 2009.

[3] S. Savola and J. Raitanen, “RFID technology and applications,” IEEE Pers. Ubiquitous Comput., vol. 15, no. 3, pp. 279–289, Jun. 2011. [Online]. Available: https://ieeexplore.ieee.org/document/5939924/

[4] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications,” IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, Oct. 2017. [Online]. Available: https://ieeexplore.ieee.org/document/8532286/

[5] B. Zhang, G. Tsudik, D. Massey, and C. Papadopoulos, “Named data networking (ndn) project,” in Proc. Eur. Conf. Netw. Commun. (EuCNC), Bologna, Italy, Jun. 2014, pp. 1–5, doi: 10.1109/EuCNC.2014.6882665.

[6] M. Almado, C. Campolo, A. Iera, and A. Molinaro, “Named data networking for IoT: An architectural perspective,” in Proc. Eur. Conf. Netw. Commun. (EuCNC), Bologna, Italy, Jun. 2014, pp. 1–5, doi: 10.1109/EuCNC.2014.6882665.

[7] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications,” IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, Oct. 2017. [Online]. Available: https://ieeexplore.ieee.org/document/8532286/

[8] M. Almado, C. Campolo, A. Iera, and A. Molinaro, “Named data networking for IoT: An architectural perspective,” in Proc. Eur. Conf. Netw. Commun. (EuCNC), Bologna, Italy, Jun. 2014, pp. 1–5, doi: 10.1109/EuCNC.2014.6882665.

[9] M. Almado, C. Campolo, A. Iera, and A. Molinaro, “Named data networking for IoT: An architectural perspective,” in Proc. Eur. Conf. Netw. Commun. (EuCNC), Bologna, Italy, Jun. 2014, pp. 1–5, doi: 10.1109/EuCNC.2014.6882665.

[10] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications,” IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, Oct. 2017. [Online]. Available: https://ieeexplore.ieee.org/document/8532286/

[11] B. Zhang, G. Tsudik, D. Massey, and C. Papadopoulos, “Named data networking (ndn) project,” in Proc. Eur. Conf. Netw. Commun. (EuCNC), Bologna, Italy, Jun. 2014, pp. 1–5, doi: 10.1109/EuCNC.2014.6882665.

[12] M. Almado, C. Campolo, A. Iera, and A. Molinaro, “Named data networking for IoT: An architectural perspective,” in Proc. Eur. Conf. Netw. Commun. (EuCNC), Bologna, Italy, Jun. 2014, pp. 1–5, doi: 10.1109/EuCNC.2014.6882665.

[13] M. Almado, C. Campolo, A. Iera, and A. Molinaro, “Named data networking for IoT: An architectural perspective,” in Proc. Eur. Conf. Netw. Commun. (EuCNC), Bologna, Italy, Jun. 2014, pp. 1–5, doi: 10.1109/EuCNC.2014.6882665.

[14] M. Almado, C. Campolo, A. Iera, and A. Molinaro, “Named data networking for IoT: An architectural perspective,” in Proc. Eur. Conf. Netw. Commun. (EuCNC), Bologna, Italy, Jun. 2014, pp. 1–5, doi: 10.1109/EuCNC.2014.6882665.
M. S. Mohd Shah et al.: Hierarchical Naming Scheme in NDN for IoT: A Review and Future Security Challenges

[63] W. Shang, A. Bannis, T. Liang, Z. Wang, Y. Yu, A. Afanasyev, J. Thompson, J. Burke, B. Zhang, and L. Zhang, “Named data networking of things (Invited Paper),” in Proc. IEEE 1st Int. Conf. Internet Things Design Implement. (IoTDI), Berlin, Germany, Apr. 2016, pp. 117–128, doi: 10.1109/IoTDI.2015.44. [Online]. Available: http://ieeexplore.ieee.org/document/7471356/

[64] D. Saxena, V. Raychoudhury, and S. Nalluri, “SmartHealth-NDNoT: Named data network of things for healthcare services,” Jun. 2015, doi: 10.1145/2757290.2757300.

[65] D. Saxena and V. Raychoudhury, “Design and verification of an NDN-based safety-critical application: A case study with smart healthcare,” IEEE Trans. Syst., Man, Cybern., Syst., vol. 49, no. 5, pp. 991–1005, May 2019, doi: 10.1109/TSMC.2017.2723843. [Online]. Available: https://ieeexplore.ieee.org/document/7990549/

[66] Z. Liu, X. Huang, Z. Hu, M. K. Khan, H. Seo, and L. Zhou, “On emerging family of elliptic curves to secure Internet of Things: ECC comes of age,” IEEE Trans. Depend. Sec. Comput., vol. 14, no. 3, pp. 237–248, Jun. 2017, doi: 10.1109/TDSC.2016.2577022.

[67] 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.

[68] B. Li, M. Ma, and R. Xia, “Hierarchical identity-based security mechanism using blockchain in named data networking,” in Proc. 3rd Int. Conf. Hot Inf.-Centric Netw. (HotICN), Hefei, China: IEEE, Dec. 2020, pp. 148–153, doi: 10.1109/HotICNS0779.2020.9350821. [Online]. Available: https://ieeexplore.ieee.org/document/9350821/

[69] S. Shannigrahi, C. Fan, and C. Partridge, “What’s in a name?: Naming big science data in named data networking,” in Proc. 7th ACM Conf. Inf.-Centric Netw., Sep. 2020, pp. 12–23, doi: 10.1145/3405656.3418717.

MOHAMMAD SHAHRUL MOHD SHAH received the Bachelor of Computer Science (B.C.S.) degree (Hons.) in network engineering and the Master of Computer Science (M.C.S.) degree in software development from Universiti Malaysia Sabah, Malaysia, in 2017 and 2019, respectively, where he is currently pursuing the Doctor of Philosophy (Ph.D.) degree in computer science. Since 2019, he has been with the Faculty of Computing and Informatics, Universiti Malaysia Sabah. In the meantime, he has joined the Department of Faculty of Computing and Informatics, Universiti Malaysia Sabah, as a Research Assistant. 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 from Universiti Teknologi Malaysia, and the Ph.D. degree in Internet infrastructures security from University Sains Malaysia. He is currently working as a Senior Lecturer 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).

ZHIWEI YAN received the Ph.D. degree from the National Engineering Laboratory for Next Generation Internet Interconnection Devices, Beijing Jiaotong University. He joined the China Internet Network Information Center (CNNIC), in 2011, where he is currently a Professor. Since April 2013, he has been an Invited Researcher with Waseda University. His research interests include mobility management, network security, and next generation internet. He is active in IETF, APNIC, ICANN RSSAC Caucus Member and published RFC8191 in IETF.

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, Malaysia (UUM), and the Ph.D. degree in advanced internet security and monitoring from University Sains Malaysia (USM). He is currently working as a Senior Lecturer with the National Advanced IPv6 Centre (NA6), USM. 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.

* * *