electronics

MDPI

Review

Detection of DoS Attacks for IoT in Information-Centric Networks Using Machine Learning: Opportunities, Challenges, and Future Research Directions

Rawan Bukhowah *, Ahmed Aljughaiman and M. M. Hafizur Rahman

Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia; aaaljughaiman@kfu.edu.sa (A.A.); mhrahman@kfu.edu.sa (M.M.H.R.)

* Correspondence: 222402836@student.kfu.edu.sa

Abstract: The Internet of Things (IoT) is a rapidly growing network that shares information over the Internet via interconnected devices. In addition, this network has led to new security challenges in recent years. One of the biggest challenges is the impact of denial-of-service (DoS) attacks on the IoT. The Information-Centric Network (ICN) infrastructure is a critical component of the IoT. The ICN has gained recognition as a promising networking solution for the IoT by supporting IoT devices to be able to communicate and exchange data with each other over the Internet. Moreover, the ICN provides easy access and straightforward security to IoT content. However, the integration of IoT devices into the ICN introduces new security challenges, particularly in the form of DoS attacks. These attacks aim to disrupt or disable the normal operation of the ICN, potentially leading to severe consequences for IoT applications. Machine learning (ML) is a powerful technology. This paper proposes a new approach for developing a robust and efficient solution for detecting DoS attacks in ICN-IoT networks using ML technology. ML is a subset of artificial intelligence (AI) that focuses on the development of algorithms. While several ML algorithms have been explored in the literature, including neural networks, decision trees (DTs), clustering algorithms, XGBoost, J48, multilayer perceptron (MLP) with backpropagation (BP), deep neural networks (DNNs), MLP-BP, RBF-PSO, RBF-JAYA, and RBF-TLBO, researchers compare these detection approaches using classification metrics such as accuracy. This classification metric indicates that SVM, RF, and KNN demonstrate superior performance compared to other alternatives. The proposed approach was carried out on the NDN architecture because, based on our findings, it is the most used one and has a high percentage of various types of cyberattacks. The proposed approach can be evaluated using an ndnSIM simulation and a synthetic dataset for detecting DoS attacks in ICN-IoT networks using ML algorithms.

Keywords: Internet of Things; denial-of-service attack; Information-Centric Network; machine learning

check for updates

Citation: Bukhowah, R.; Aljughaiman, A.; Rahman, M.M.H. Detection of DoS Attacks for IoT in Information-Centric Networks Using Machine Learning: Opportunities, Challenges, and Future Research Directions. *Electronics* **2024**, *13*, 1031. https://doi.org/10.3390/electronics13061031

Academic Editors: Abdussalam Elhanashi and Pierpaolo Dini

Received: 29 January 2024
Revised: 28 February 2024
Accepted: 28 February 2024
Published: 9 March 2024

1. Introduction

With the rapid development of new technologies, the Internet environment is changing accordingly. The Internet of Things (IoT) is one of those technologies. It creates new challenges including content, service, and device-naming challenges that aim to connect a massive number of heterogeneous devices. Consequently, there is a need for an infrastructure in which the content is the main element [1]. The IoT is an ecosystem, and most of its applications follow content-oriented usage patterns. The IoT is a vast network of interconnected devices that collect and exchange data. Most IoT applications follow content-oriented usage patterns, meaning that users are primarily interested in obtaining specific data items, rather than communicating with specific devices. The Information-Centric Network (ICN) is a new networking paradigm that can improve the performance and security of IoT applications. The ICN replaces the traditional host-centric networking approach with a content-centric approach, meaning that users request specific data items, rather than communicating with specific devices. The ICN offers a number of benefits for IoT applications, including content-based security, reduced network traffic, improved performance, retrieval of the content fast, multi-casting, and in-network caching [2,3].

IoT technology plays a key role in our daily lives as the IoT has opened new doors for better communication and better ways to deal with the massive data obtained through these heterogeneous devices [1]. Based on the application domain, IoT sensors can be utilized for monitoring medical services, smart homes, smart environments, smart cities, and smart enterprises, as shown in Figure 1. Consequently, these applications have led to an increase in interconnected devices, including smart and sensing devices. With technology development, IoT applications surround us from every side. For example, in healthcare, there is a huge interest in using IoT as it reflects good services for patients and hospitals in general. Wireless sensor networks (WSNs) and wireless body area network (WBANs) are essential components used in healthcare environments [4]. The implementation of the IoT has led to many security and privacy challenges [5]. Therefore, nowadays the IoT is one of the main focuses of research across the world.

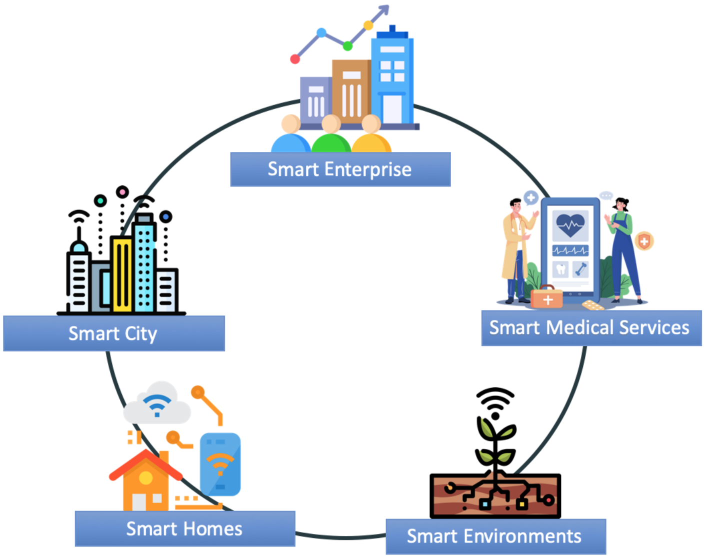

Figure 1. IoT applications.

The goal is to make IoT resources accessible anytime, anywhere, and by anything in a secure manner. The old Transmission Control Protocol-/Internet Protocol-based networks (TCP/IP) appear to have serious problems in the IoT field, so to overcome these problems we need a network with a big capacity to address these issues. In light of this, the ICN architecture is an alternative solution to the oldest TCP/IP networks. The ICN secures content itself instead of the communication channel, so it replaces the host-centric model with the content-centric model [6]. In the traditional TCP/IP protocol, it is not possible to connect a massive number of devices to the system. In contrast, the ICN can accommodate a vast number of devices. Therefore, network routing, stability, scalability, and mobility management have been enhanced for various IoT applications through the ICN [3].

Moreover, ICN architectures consist of Named-Data Networking (NDN), Content-Centric Networking (CCN), the Publish–Subscribe Internet Routing Paradigm (PSIRP), Data-Oriented Network Architecture (DONA), and Network of Information (NetInf) [7]. The ICN enhances the user experience with security, privacy, and access controls. However, it also introduces new challenges. Therefore, the challenge of this paper is to define and present all possible issues, attacks, and cybersecurity problems that take place in the ICN architectures of the IoT. Another challenge is to give potential solutions, using techniques to defend against defined cybersecurity problems.

There are several techniques to detect and mitigate DoS attacks. Some of the mitigation techniques have been suggested by [8], including artificial intelligence technology, probabilistic and statistical methods, and miscellaneous approaches. These methods are significant methods to detect and mitigate DoS attacks such as the interest flooding attack (IFA). Other methods are recommended by [9], including the statistical approach, heuristic approach, machine learning (ML), and deep learning (DL). Consequently, there are various anomaly-based attack detection techniques to use. Table 1 shows a comparison between ML, DL, and statistical approaches based on their features and limitations.

Table 1. Comparison between mitigation techniques.

Techniques	Features	Limitations
Statistical approach	• These statistical rests are used to prove that the observed pattern and expected pattern is different based on historical data • Real-time detection • Low false positive rate	• Misclassification • Very complex • Accuracy depends on the mathematical model
ML	• Can learn complex traffic patterns quickly • Can automatically extract relevant features from network traffic data • High detection accuracy • Real-time detection	• Long training time • Need large dataset for better results
DL	• Can extract features of supervised and unsupervised learning • Can directly process raw data	• Data dependency • May leads to overfitting • Very complex • Computational overhead • Need large dataset for better results

Detecting cyberattacks is challenging, especially in ICN networks, as it is a new concept, and based on recent research there are various types of attacks, including DoS attacks, that successfully breach the network. Therefore, it is critical to detect these attacks and develop better methods to minimize the likelihood of a system being compromised. According to the papers that we have reviewed, ML technology is considered an efficient way to address ICN-IoT challenges. However, none of these papers applied ML to detecting DoS attacks in the ICN-IoT network. Therefore, our proposed paper combines these technologies to enhance security.

1.1. Problem Statement

In the contemporary IP-based network infrastructure, DDoS attacks represent a pervasive threat, inflicting substantial harm upon the network's functionality and integrity. However, the ICN exhibits promising capabilities in thwarting numerous prevalent DoS attack vectors. Common DoS attacks afflicting IP-based networks include reflection attacks, bandwidth depletion, and black-holing via prefix hijacking [10]. Initially, there was a prevailing belief that the IoT realm could withstand DDoS attacks due to the inherent design of NDN. This belief was challenged upon the discovery of specific DoS attack vectors, such as IFAs and state-based attacks. Additionally, the proliferation of content requests and user-generated names has led to the overloading of forwarding information base (FIB) and pending interest table (PIT) structures [11]. Consequently, the integration of the IoT with the ICN has emerged as a focal point for researchers, necessitating a deeper exploration of the associated challenges and vulnerabilities.

DoS represents a significant security concern within the ICN-IoT paradigm, where attackers exploit vulnerabilities to deplete network resources by flooding malicious content over the infrastructure. For example, IFAs involve a large volume of diverse or identical interest packets, often containing non-existent data. The aim of those packets is to overwhelm the resources of the data producer or the entire network infrastructure [10], thus causing significant disruption and damage within the ICN-IoT environment.

To mitigate the impact of such attacks, various methods have been proposed. The token bucket with per-interface-fairness approach, for instance, restricts the number of outgoing interest packets by limiting tokens associated with the outgoing interface. Similarly, the satisfaction-based interest acceptance method allocates tokens to incoming interfaces based on their interest–satisfaction ratio. Another strategy involves disabling PIT exhaustion. However, these mitigation methods exhibit certain limitations and may not be sufficiently effective in practice [10]. Consequently, there is a pressing need for more robust and efficient solutions to bolster the resilience of IoT-ICN integration against DoS attacks. The proposed detection system, leveraging ML technology, aims to provide a more effective solution. By harnessing ML algorithms and advanced analytics, our proposed approach endeavors to enhance the security posture of ICN-integrated IoT environments, offering proactive threat detection and mitigation capabilities.

1.2. Why ICN for IoT?

The IoT deals with numerous and diverse networked devices and complex traffic patterns that issue unique challenges. Applying ICN principles in this context creates new opportunities [12]. Recently, the ICN has gained recognition as a promising networking solution for the IoT. In the context of the IoT, the data generated by smart devices are treated as content. This means that network users can request IoT data without needing to know their specific sources, like sensors or actuators. The ICN approach focuses on content names rather than network addresses, eliminating the need for end-to-end session requirements.

The ICN offers several advantages to the IoT, including improved data retrieval, reduced latency, an efficient receiver-driven design, request aggregation, and support for mobility and multicast at the network layer. One additional feature is in-network caching, which enhances data availability by caching the requested contents near users. This technique reduces traffic near the IoT data publisher and leads to lower energy requirements [2]. Consequently, the ICN is often considered more suitable for IoT applications than traditional IP-based networking. Moreover, the ICN provides robust content-based security and encryption, ensuring data integrity and authenticity [13]. The ICN also addresses issues in the IoT by using content-based naming and a name-resolution system (NRS). In addition, within the application layer, there are various trust models implemented to serve multiple purposes, such as content encryption and security [13].

The remainder of this paper is organized as follows. In Section 2, we discuss IoT three-layer architectures, ICN architectures, related attacks in the ICN and the IoT, and the importance of integrating the ICN with the IoT. Section 3 discusses machine learning techniques in the ICN-IoT environments. Section 4 conducts a comprehensive analysis of related studies. Section 5 presents results and discussions based on the ICN and the IoT. Section 6 includes the recommendation and future research directions. Section 7 concludes the paper.

2. Background

2.1. Internet of Things (IoT)

The IoT refers to the "Internet of things". The IoT is a technological paradigm that revolves around the seamless integration of computational devices and physical objects. These objects are equipped with unique identifiers, sensors, and the capability to collect, process, and share data. Regarded as one of the most groundbreaking technological advancements in recent years, the IoT has far-reaching implications in various domains. IoT systems encompass a wide range of applications. They find their place in automated vehicles, where they enhance safety and efficiency, in the energy sector, optimizing the supply transmission, distribution and consumption of energy and in surveillance systems, and exemplified by the deployment of drones for enhanced monitoring and security. However, the influence of the IoT extends far beyond these sectors. It has infiltrated academic institutions, industries, factories, agricultural settings, healthcare organizations, and more [14]. Nowadays, IoT security is a big concern and the security vulnerabilities of IoT are unique because they are complex and heterogeneous in technology and data.

2.1.1. IoT Applications

The IoT comprises a wide range of applications that have increased very rapidly. These applications require additional security support from various new technologies. Below, some of the security applications in the IoT are discussed:

- Smart medical services: This includes monitoring respiration, drug delivery systems, body position, quality of sleep, and early detection of illness [4].
- Smart homes: For example, a smart camera captures an image around the door and then sends it to the owner when someone acts in unusual behavior near the door [4].
- Smart environments: This includes anything that is connected to and affected by humans, animals, and plants. These include air quality and water quality monitoring, natural disaster monitoring, and smart farming [4]. Moreover, smart environments include monitoring the level of snow in high-altitude regions, pollution monitoring, early detection of earthquakes, fire detection, and landslides prevention [15].
- Smart cities: This involves emerging computation and communication resources. Although, the goal is to increase the quality of life of people, it comes with a lot of challenges. For example, Air Tag from Apple could be used to enable parents to track their children; this feature will become risky if it is hacked because it breaches the privacy of citizens [15].
- Smart enterprises: These organizations can maintain real-time shipment tracking in transportation and logistics areas and smart farming under energy and production and resource management [4].

2.1.2. IoT Layers

Various architectures have been proposed by researchers, the most fundamental architecture developed is the three-layer model (Figure 2). Every layer has many security issues and attacks that can target each layer.

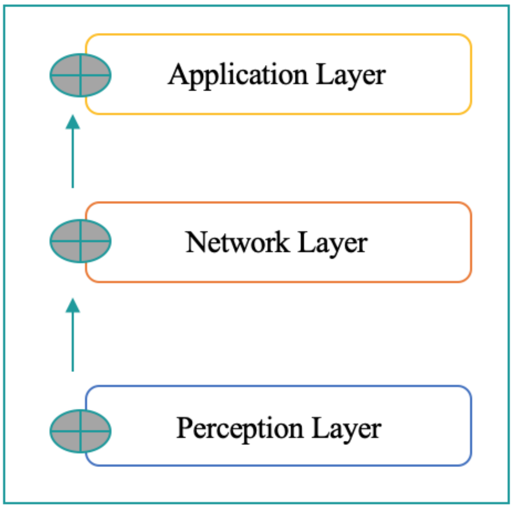

Figure 2. The three layers of the IoT.

Denial-of service attacks in the IoT layer: The IoT is a rapidly growing network of physical devices that are connected to the Internet and can collect and exchange data. While the IoT has the potential to revolutionize many industries and aspects of our lives, it also introduces new security challenges. One of the most significant challenges is DoS attacks. DoS attacks aim to overwhelm the target system with too much traffic, rendering it unavailable to legitimate users. These attacks can be particularly effective against IoT devices due to their often poor security and limited resources. IoT systems are structured into three layers: the perception layer, the network layer, and the application layer. According to a recent report by Cloudflare, in 2023, the number of DoS attacks targeting the network layer increased by 85% compared to 2022 [16]. The most targeted industries were the telecommunications industry, gaming and gambling companies, and then the information technology and services industry. Consequently, DoS attacks against the IoT are a serious concern and may have a significant impact on both businesses and individuals, potentially resulting in financial losses and reputational damage [17]. DoS attacks target IoT layers, including:

- Perception layer DoS attacks: In this layer, DoS attacks target sensors and other devices, aiming to send invalid data or overwhelm traffic within IoT devices [18].
- Network layer DoS attacks: In this layer, the routers, switches, and other networking devices are targeted by DoS attacks in order to disrupt the communication between the perception layer and the application layer.
- Application layer DoS attacks: In this layer, applications are targeted. DoS attacks aim to overwhelm the applications with traffic or to send them invalid data [18].

2.2. Information-Centric Network (ICN)

The ICN has been proposed as a future internet architecture. Unlike IP-based networks, which rely on host addresses for communication, the ICN adopts a content-centric communication model. In this model, the focus is on the content itself, instead of host addresses. The ICN's objective is to separate content from its hosting locations, allowing ICN forwarders to cache content within the network and fulfill subsequent client requests without the need to forward them to the original producer [7].

In the ICN, content discovery and delivery operate in a receiver-driven manner, as shown in Figure 3. It all begins when a consumer initiates a content request, referred to as an interest packet, which contains the name of the desired content. This interest packet is routed hop-by-hop, based on the content name, until it reaches the content producer. The producer can be either the original data source or an intermediate node that stores the requested content. Moreover, the data packet is sent back as a response along the reverse path of the interest to fulfill the request. Unlike host-based networks, on which securing the communication channel between hosts is paramount, the ICN employs a content-centric security model. This model directly secures the content itself instead of the communication channel [6].

Implementing the ICN in wireless environments can cause various security concerns caused by the inherent characteristics of wireless communication and the content-centric communication model of the ICN. These issues include content name attacks, which can impact user privacy, the management of access control rules tied to content names, the establishment of trust in wireless settings, and the authentication of data originating from content stores [6].

2.2.1. ICN Architectures

As shown in Figure 4, which illustrates the timeline of ICN projects, throughout the years, different countries have supported different ICN projects. The United States supported the following projects: Content-Centric Networking (CCN), Named-Data Networking (NDN), MobilityFirst, and ICE-AR. In contrast, the European Union funded different ICN projects, such as the Publish–Subscribe Internet Technology (PURSUIT), Scalable and Adaptive Internet Solutions (SAIL), Content Mediator Architecture for Content-Aware Networks (COMET), CONVERGENCE, and ANR Connect. Multiple countries collaborated to fund the following ICN projects: GreenICN and ICN-2020. The architectures of some of the above projects are discussed below.

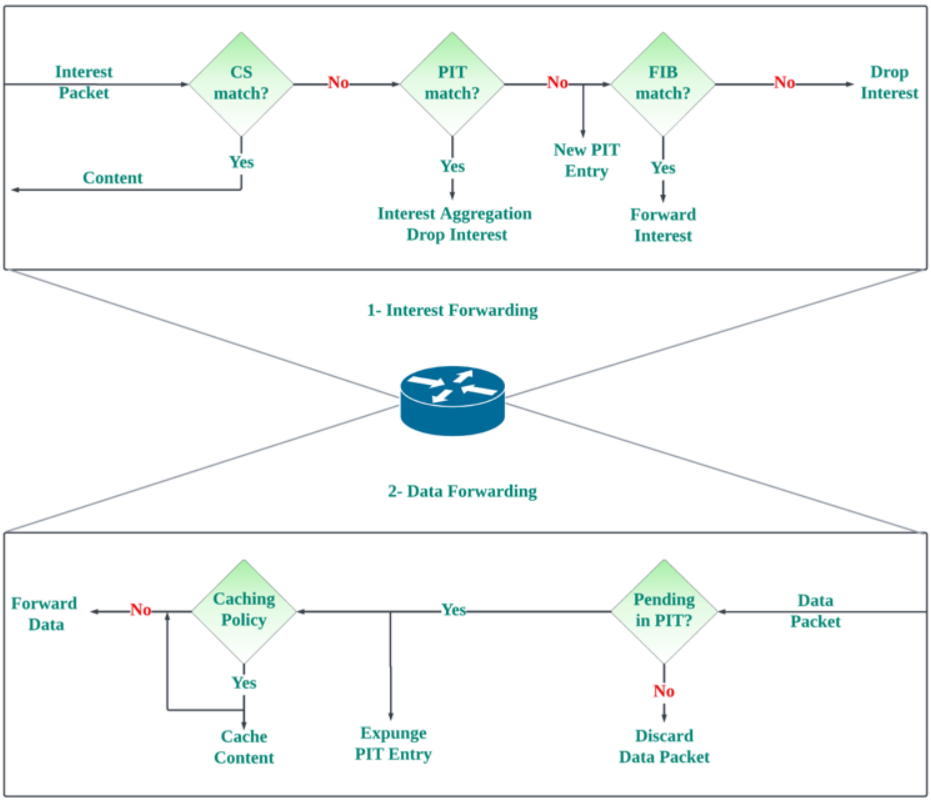

Figure 3. ICN process.

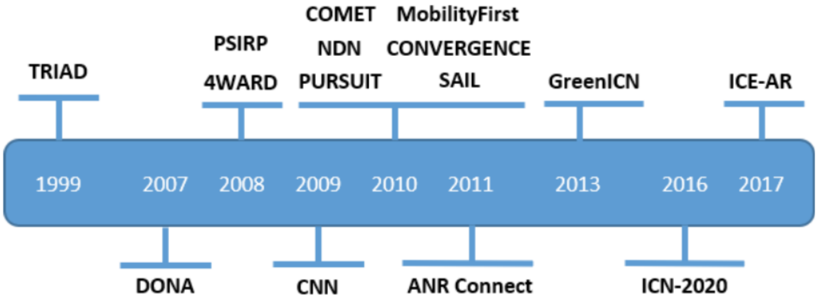

Figure 4. Timeline of ICN projects [6].

Data-Oriented Network Architecture (DONA): DONA was marked as the first project in the development of the ICN, as it became the first ICN architecture to reach completion. DONA was an evolution of TRIAD's foundational design principles, particularly transforming from hierarchical URLs to a flat naming scheme, which makes DONA no longer reliant on a single host to serve content [19]. In the DONA scheme, content names are comprised of a cryptographic hash of the publisher's key and an object ID assigned by the publisher. This naming scheme ensures uniqueness within the publisher's domain [18].

Publish–Subscribe Internet Technology (PURSUIT): PURSUIT is an initiative within the European Union. This project follows the Publish–Subscribe Internet Routing architecture like its predecessor. This architecture features a comprehensive publish–subscribe protocol stack, instead of the conventional IP protocol stack. In the context of PURSUIT, its core functions encompass three key aspects: rendezvous, topology management, and forwarding. In 2008, PSIRP was introduced, and around the same time, another promising project known as Architecture and Design for the Future Internet (4WARD) also emerged [18].

The Network of Information (NetInf): This network was started in the 4WARD architecture. NetInf uses a publish–subscribe scheme as well as flat naming, which maps names to locators. Content is retrieved by having the publisher first publish its data objects to the network, and NRS stores the name and locator mapping. Data can be stored in cache in many places, and hence, can be available to many locators. When a subscriber requests the content, the routing forwarders deliver the data [18].

Content-Centric Networking (CCN): CCN and NDN exhibit similarities in their architectural design, encompassing elements such as a hierarchical naming scheme, content caching, and named content routing.

Named-Data Networking (NDN): CCN was introduced in 2009 by researchers at the Palo Alto Research Center. In CCN, known as a data-named communication architecture, the packet is addressed with content names instead of locations. This procedure was also applied to other objects, with NDN being the most famous one. They are similar, a client requests content by sending an interest packet into the network with the content's name. In the NDN network, the subscribers send the interest packet to request data objects. This interest packet goes to the content router (CR) then it will be forwarded hop-by-hop across CRs. A CR contains three data structures: content store (CS), FIB, and PIT. The CR stores the content that travels around the interface. FIB storage also stores pairs of names and then forwards them to the target address. Consistently, interest packets are forwarded to the destination based on the requested content. Moreover, the PIT, as well as FIB, stores pairs of names in the interface that request the content. It will then be used to propagate data objects to the subscriber. NDN is the chosen architecture for the project's implementation within the field of the ICN. Content storage has consistently created challenges, including managing large-scale network caches, determining what content to discard when new content arrives, and efficiently storing content in the cache [18]. Figure 5 illustrates the components of NDN's interest packet and data packet.

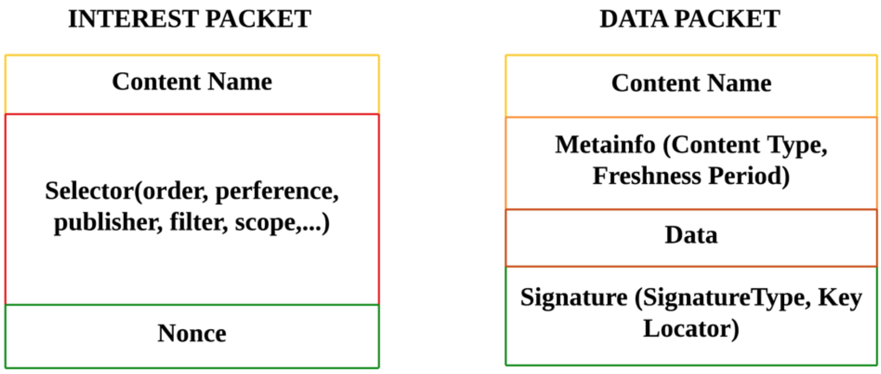
INTEREST PACKET
Content Name
Selector(order, perference, publisher, filter, scope,...)
Nonce
DATA PACKET
Content Name
Metainfo (Content Type, Freshness Period)
Data
Signature (SignatureType, Key Locator)

Figure 5. NDN's interest packets and data packets.

2.2.2. Taxonomy of DoS Attacks in the ICN

The ICN poses numerous security challenges that require attention. It introduces new types of attacks that did not occur previously. Moreover, ICN environments may also be susceptible to attacks commonly observed in other networking environments. The ICN is considered a new architecture in terms of naming, routing, and caching. DoS attacks aim to disrupt or disable the normal operation of a network or service. DoS attacks can be launched against a variety of targets, including servers, websites, and routers. In ICNs, DoS attacks can be particularly disruptive due to the reliance of the ICN on secure and reliable communication between network entities. Figure 6 illustrates the list of attacks that can target the ICN.

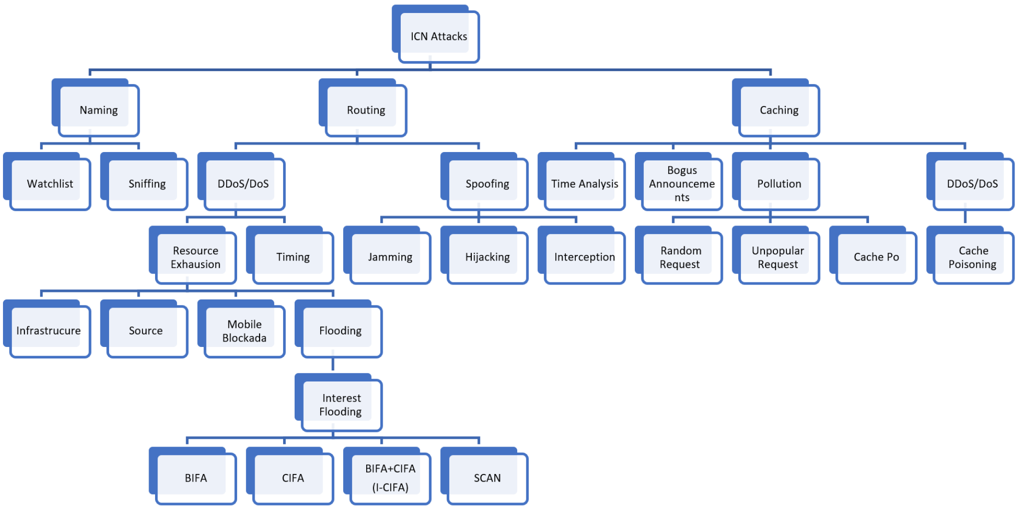

Figure 6. Taxonomy of ICN attacks in the ICN.

Naming-Related Attacks

In the naming domain, the biggest concern is that the ICN will face a threat with respect to privacy, such as a sniffing attack, in which attackers try to monitor Internet usage. In naming-related attacks, the watchlist attack occurs when attackers attempt to prevent the distribution of particular content. This is achieved by blocking the delivery of the content and potentially identifying who is requesting it [20].

Routing-Related Attacks

Attacks that belong to routing include DoS attacks, spoofing, timing, and jamming attacks. The attackers' goal is to cause unwanted traffic flows and DoS. Other attacks, including infrastructure and flooding attacks, try to exhaust the resources such as memory and processing power, that are used to support, maintain, and exchange content states.

Flooding is a special type of attack that only happens in the ICN environment. There are four types of IFAs: basic IFA (BIFA), collusive IFA (CIFA), smart collaborative attack in NDN (SCAN) and BIFA+CIFA [20]. These types of attacks aim to disrupt the network functionality of the ICN by flooding it with a large number of illegitimate interest messages to overwhelm the network's infrastructure. These attacks may cause network congestion, resource depletion, DoS, and increased energy consumption in IoT devices [21].

Caching-Related Attacks

Caching plays a crucial role in the ICN by improving infrastructure performance through receiver-driven caching. The goal of this approach is to offer users the nearest available copy. Consequently, the ICN is vulnerable to any actions that pollute or corrupt the caching system. Notably, cache pollution attacks and interest poisoning attacks pose substantial threats to the effectiveness of ICN caching [20].

3. Machine Learning Techniques in the ICN-IoT

The ICN is a new networking paradigm that only focuses on the information instead of the location of the information, so it is well-suited to the IoT. However, ICN-IoT networks are vulnerable to various attacks, including DoS, malware, and data breaches. ML is an optimal solution for detecting anomalies in ICN-IoT networks in order to mitigate these attacks. ML algorithms can be trained on historical data to learn normal network behavior. Then, they can monitor network traffic against anomalies. ML-based anomaly detection systems are very helpful in the detection of a variety of attacks, such as DoS attacks, malware attacks, and data breaches [22]. There are various ML techniques; each of them has its advantages and limitations, so we should choose between them based on the specific requirements of the ICN-IoT network. The most common techniques include the following:

- Unsupervised learning: In unsupervised learning algorithms, labeled data for training is not required. Instead, this type focuses on analyzing unlabeled data to identify patterns and anomalies. This approach is particularly useful in ICN-IoT networks.
- Supervised learning: In supervised learning algorithms, labeled data for training is required. Therefore, categorizing labeled data as either normal or abnormal, and identifying real-time network traffic as either normal or abnormal. This approach can be beneficial in detecting anomalies in ICN-IoT networks.
- Semi-supervised learning: In semi-supervised learning techniques, ML algorithms can be trained using a small amount of labeled data along with a large amount of unlabeled data. Since labeled data may be scarce, this approach is useful in ICN-IoT networks [22].

3.1. Supervised Learning Algorithms

There are two fundamental types of machine learning algorithms: supervised and unsupervised. Supervised algorithms employ pre-labeled (classified) objects to predict the class of objects. In contrast, unsupervised algorithms aim to discover the natural grouping or patterns within unlabeled, new, and unseen objects. Supervised learning algorithms can be adapted to the unique characteristics of NDN-IoT environments. By tailoring the features and labels to capture relevant aspects of the network traffic, these algorithms can be customized for specific IoT scenarios. There are three types of classifier algorithms.

3.1.1. K-Nearest Neighbor (KNN)

KNN is valuable for classification as it does not assume underlying data distributions, making it a non-parametric and lazy learning algorithm. Non-parametric statistics operate under the assumption that there is no predefined data distribution [23]. In addition, the KNN algorithm takes as input the k-nearest training samples in the feature space. The accuracy of this algorithm can be significantly enhanced by normalizing the training data [24]. Furthermore, in KNN, the critical factor is the number of nearest neighbors [23].

3.1.2. Support Vector Machine (SVM)

The SVM framework serves as an intersection between machine learning and embedded systems. SVM functions as both a linear and nonlinear classifier, acting as a mathematical function capable of distinguishing between two types of objects, categorized as classes [23]. The reason for utilizing the SVM algorithm is its efficient capability to differentiate between the characteristics of traffic flow in normal and abnormal scenarios [24].

3.1.3. Random Forest (RF)

RF is a supervised classification algorithm that constructs a random forest. The accuracy of the results improves with an increase in the number of trees in the forest [23]. In addition, during the training phase, RF builds numerous decision trees and provides an output based on the mode of classes (for classification) or the mean prediction (for regression) of the individual trees [24].

Several ML algorithms are used for attack detection in ICN-IoT. Related studies indicate that KNN, SVM, and RF yield optimal results and are popularly used. Kumar et al. [25] evaluated various shallow ML algorithms including SVM and KNN, showing their effectiveness in attack detection. In [8], the authors highlighted SVM as the primary method, using Jensen–Shannon (JS) divergence, for detecting IFA attacks. Consistently, the parameters utilized include the number of incoming and outgoing data packets and interest packets, alongside the size of the PIT entries. Furthermore, classification metrics such as accuracy = $\frac{TP+TN}{TP+TN+FP+FN}$, precision = $\frac{TP}{TP+FP}$, recall (sensitivity) =$\frac{TP}{TP+FN}$, and F-measure are commonly employed for evaluation purposes [8,25].

ML is a subset of AI that focuses on the development of algorithms. In the context of IFA over the NDN platform, three popular ML algorithms, which are SVM, RF, and KNN, have been highlighted in the papers that either reviewed or tested IFA. The literature has explored several ML algorithms, including neural networks, decision trees (DTs), clustering algorithms, XGBoost, J48, multilayer perceptron (MLP) with backpropagation (BP), deep neural networks (DNNs), MLP-BP, RBF-PSO, RBF-JAYA, and RBF-TLBO. Researchers compare these detection approaches using classification metrics such as accuracy.

The reviewed studies indicate that SVM, RF, and KNN demonstrated superior performance in IFA detection. In the KNN method, attacks were localized with 98.35% accuracy. As for the SVM, it achieved a detection accuracy of 99.4%. Moreover, RF had the best performance in terms of accuracy, precision, and recall. Overall, the results highlight the effectiveness of the KNN, SVM, and RF models compared to other alternatives [25]. Consistently, the reviewed studies considered several parameters, including the number of incoming and outgoing data packets and interest packets, alongside the size of the PIT entries [8].

In addition, to deploy a proposed project using ML several key stages are essential, as shown in Figure 7. These start with the processing phase, which includes ndnSIM to train the system and dataset preprocessing to clean and transform data. Also, there is a need to check and remove any unnecessary or null values because ML algorithms have a difficult time handling them, which can lead to incorrect results. The next stage is feature selection, which also includes feature preprocessing. In this stage, the initial dataset should be built. After the features are selected, the dataset is divided into two subsets: the training subset and the testing subset. By selecting the right testing and training data, classification accuracy can be improved [26]. The training data are the set of instances trained on the model, while the test data are used to determine the model's ability or execution. Classification determines whether the information belongs to a normal class or a DoS attack. To achieve the best classification approach, a variety of algorithms, such as KNN, SVM, and RF, should be compared.

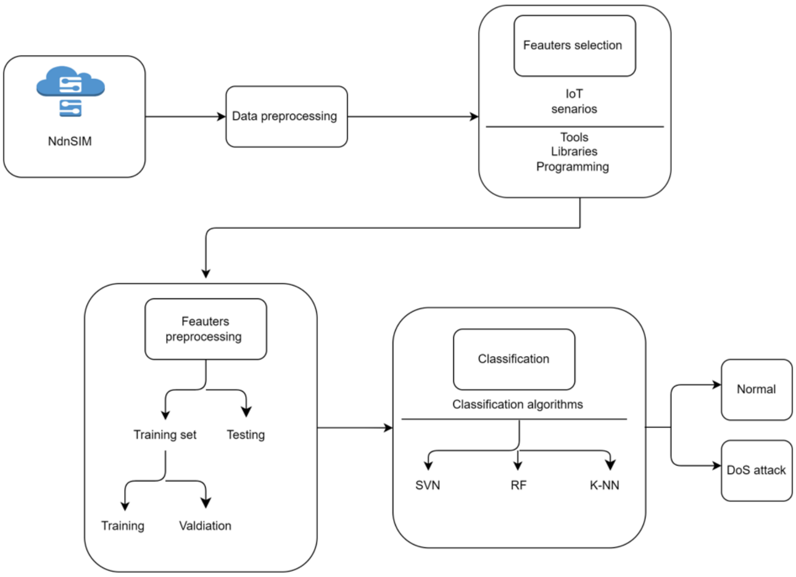

Figure 7. System architecture.

4. Related Work

In this section, we review several research papers related to security threats associated with IoT and ICN technologies. The research addresses its aims by undertaking a systematic review of the literature, following the PRISMA 2020 protocol. The procedures involve collecting, reading, selecting, and analyzing various papers' results using Google Scholar and the Saudi Digital Library databases.

4.1. Threats on the IoT

Samundra et al. [27] presented security and privacy challenges related to the IoT in general and then described each layer of the IoT architecture, with its related security issues. These IoT layers are the perception layer, network layer, middleware layer, and application layer. The paper suggested several solutions to address the challenges in the IoT.

Azzam et al. [28] reviewed threats and attacks that are related to IoT and classified them according to the three layers of the IoT: perception or the physical, network, and application. In addition, the paper explained mitigation techniques that could be applied to IoT threats and attacks. Some of these countermeasure techniques are encryption, access control, AI, and blockchain technology.

Waseem et al. [29] presented the threats to the IoT, as well as the challenges, risks, and security requirements for the IoT in general and each of its layers. They also highlighted most of the well-known and generic attacks on all types of IoT layers, such as DoS attacks in the network layer, SQL injection in the application layer, and battery drainage attacks in the physical layer. In addition, the paper reviewed and analyzed SDN as a network that can deploy an IoT architecture. The paper suggested solving security issues through ML.

Pintu et al. [5] reviewed the challenges, risks, and issues of the IoT from different perspectives. The authors also discussed the four layers of the IoT that have been described in detail, along with the main attacks against each of them. Moreover, the paper presented relevant countermeasures and solutions. The proposed solutions include PUF-based, blockchain, ML, and others. Finally, the paper discussed the pros and cons of these security solutions to facilitate the process of presenting future recommendations.

Thalawattha et al. [30] reviewed and analyzed security issues and requirements in the IoT to defend against IoT attacks and identified current vulnerabilities. Moreover, the paper specified attacks for each layer of the IoT and discussed the challenges in the healthcare and education fields and more. The current security techniques and their challenges were also discussed.

Dhuha et al. [31] provided a literature review to clarify related works and discuss IoT security and privacy issues. The paper then presented security attacks as layer-wise attacks and attack taxonomy perspectives and analyzed them based on the IoT layers. In addition, the paper suggested solutions and stated strategies against these attacks.

Muhammed et al. [32] proposed a comprehensive survey of security issues in the IoT. This paper presented an overview of different layers in the IoT and classified the attacks on each layer. Furthermore, mitigation techniques for these attacks were reviewed. The paper suggested new IoT architecture layers to overcome these issues, the security mechanisms used are authentication, encryption, decryption, and encrypted hash.

Garima et al. [33] discussed a comprehensive study and undertook a literature review to determine threats and security aspects for all IoT layer types. They also explained the various parameters of IoT protocols, including common characteristics, limitations, advice, and countermeasures. In addition, this paper focused on exploring all related IoT security issues concerning various layers.

Muath et al. [15] reviewed IoT applications, limitations, and security issues related to each domain. In addition, it provided a survey on IoT security, its threats and vulnerabilities, its privacy challenges, and corresponding countermeasures. The paper presented the Internet of Vulnerabilities (IoV) as the growth of the IoT in our daily lives has increased. Furthermore, it discussed various cybersecurity attacks, threats, and vulnerabilities based on confidentiality, integrity, and availability. Finally, mitigation and countermeasures to these security concerns were also discussed in the paper.

Shantanu et al. [34] analyzed security issues of different layers in the Industrial Internet of Things (IIoT) architecture. In addition, they presented a list of IIoT security requirements; then, the paper looked at future research directions and countermeasures against IIoT issues. Table 2, below, presents a summary of the addressed threats for every layer of the IoT.

Table 2. Summary of addressed threats for every layer of IoT.

Author	Publication Year	Application Layer Threats	Network Layer Threats	Perception Layer Threats
Samundra et al. [27]	2022	Data access control issues, authentications issues, data protection and recovery issues, phishing attacks problems, vulnerabilities, clone attack	Cluster security issues, DoS, spoofed and replayed routing information or altered them	Fake or node capture, mass node authentication, key management mechanism, cryptographic algorithm
Azzam et al. [28]	2022	Jamming physical attack, injection attacks, cloning attacks, eavesdropping and tampering	DoS attacks, DDoS attacks, MITM attacks, sinkhole attack, traffic analysis	Phishing attacks, malware attacks, DoS/DDoS, buffer overflow attacks, spyware attacks
Waseem et al. [29]	2020	Malicious code, weak application security cross-site scripting, eavesdropping and MITM	DoS attacks (collision attack and channel congestion), escalating frame counter value, spoofing like battery exhaustion attack, message alteration attacks, replication of nodes and storage attack	Eavesdropping, battery drainage attack, hardware malfunctioning, malign data injection, node cloning, gaining unauthorized access to the device
Pintu et al. [5]	2022	Spyware and adware, Trojan horse, Botnet attack, DoS, brute-force password attack, firmware hijacking, malicious scripts, phishing attacks, worms, virus	Traffic analysis attacks, RFID spoofing, RFID cloning, RFID unauthorized access, MITM, DoS, sinkhole attack, routing information attack, Sybil attack, replay attack, hello flood attack, blackmail attack, blackhole attack, wormhole attack, grayhole attack	Node jamming, physical damage, node tampering, social engineering, malicious node injection, sleep deprivation attack, RF interference, tag cloning, eavesdropping, tag tampering outage attack, object replication, hardware Trojan
Thalawattha et al. [30]	2021	DoS attacks	DoS attacks	Leakage of privacy, sniffing service information manipulation, lack of encryption, weak default password, the rise of Botnets
Dhuha et al. [31]	2020	Malicious code injection, DoS attack, spear-phishing attack, sniffing attack, overwhelm, reprogram	Sybil attack, sinkhole attack, sleep deprivation attack, DoS attack, malicious code injection, MITM attack, traffic analysis, passive monitoring, eavesdropping	Unauthorized access to tags, tag cloning, eavesdropping, spoofing, RF jamming, timing attack, replay attack, node capture attack, malicious node injection attack, brute-force attack, radio interference, tampering
Muhammed et al. [32]	2018	Cross-site scripting attack, malicious code injection attacks, the ability to deal with mass data spear-phishing, social engineering	DoS attacks, MITM attacks, storage attacks, exploit attacks	Eavesdropping, node capture, fake node injection, replay attack, timing attack
Garima et al. [33]	2021	DoS attack, data leakage, data transit attacks	Routing attacks, data transit attacks	Node tempering, impersonation
Muath et al. [15]	2020	DoS attacks, software vulnerabilities, malicious virus/worm/Trojan horse, code injection, buffer overflow, phishing attack, spyware, malicious scripts, sensitive data manipulation, data leakage	Spoofing attacks, selective forwarding, DoS attacks, MITM attacks, sinkhole attacks, packet replication attacks, wormhole attacks, Sybil attacks, traffic analysis, sniffing attacks, routing information attacks	False data injection attacks, eavesdropping, interference, social engineering, node jamming attack, malicious node injection, sleep deprivation, tag cloning
Shantanu et al. [34]	2021	Injecting malicious codes, MITM attacks, DoS/DDoS attacks	Session hijacking, blackhole attack, wormhole attack, DNS spoofing, DoS/DDoS attacks, MITM attacks	Jamming attack, eavesdropping

4.2. Threats to the ICN

Bengt et al. [35] observed and compared ICN architectures, including CCN, PSIRP, NetInf, and DONA. Under these approaches, some challenges and issues for the ICN were discussed. One of the main issues is security; mobility, privacy, and scalability are also concerns. The implantation challenges for implementing the generic building blocks of these four approaches were introduced in the paper, and deployment issues were also discussed. Finally, the remaining challenges were discussed.

Boubakr et al. [6] presented all related security issues of deployed ICNs in wireless environments, especially for NDN architecture. The paper discussed attacks that may take place on the ICN network and its applications. A variety of issues and attacks were focused on in the paper, including security risks with attacks on content names, a list of attacks in the ICN, issues that relate to the design of NDN, such as unclear interest aggregation and illegal content caching, as well as some other attacks, such as DoS, content poisoning, and more. In addition, the paper provided solutions and countermeasures to present issues and attacks.

Reza et al. [7] provided an overview survey of related works about security and privacy issues in the ICN. This paper focused on three areas of security threats that review DoS, content poisoning, and cache pollution attacks. Then, it discussed privacy risks that concern user privacy and anonymity, content privacy, and name and signature privacy. At the end, the paper reviewed all available access control mechanisms.

Muhammed et al. [36] presented a new scheme called the secure distribution of protected content (SDPC) to ensure that only authenticated consumers can access the content. Furthermore, the paper presented all relevant security issues in the ICN by performing a formal analysis using BAN logic Scyther implementation.

Rao et al. [37] observed that the CCN is the extraction of the ICN so it analyzes the basic CCN principles and proprieties of three areas: caching, mobility, and security. This paper presented a quantitative comparison and discussion of related studies. In addition, the analysis of CCN security schemes and relevant risks was included in the paper. Last, DoS attacks were discussed in detail.

Yong et al. [38] presented an architecture, and then, examined content security to classify the security concerns of NDN content, including naming, caching, and routing-related attacks, as the paper gives all possible solutions to these problems. Moreover, the paper suggested some digital signature schemes, such as network coding signatures. Table 3, below, presents a summary of ICN-related work.

Table 3. Summary of classification of ICN architectures based on related attacks.

Author Publication	Year	Classification of ICN Architectures	Related Attacks for Each Architecture
Bengt et al. [35]	2012	NetInf	Human friendly issues, data integrity issues
		CCN	security issues
		PSIRP	Human readable names issues (DoS attacks)
		DONA	Multiple names issues
Boubakr et al. [6]	2021	NDN	Passive attack, cache pollution attack, DoS attack, content poisoning attack

Table 3. *Cont.*

Author Publication	Year	Classification of ICN Architectures	Related Attacks for Each Architecture
Reza et al. [7]	2018	Applicable to all ICN architectures	DoS attack
		Applicable to all ICN architectures	Content poisoning attack
		Applicable to all ICN architectures	Cache pollution attack
		Feasible for all ICN architectures that employ caching, so the PSIRP and PURSUIT architectures are excepted	Timing attack
		Only applicable to CCN and NDN architectures	Discovery and protocol attacks
Muhammed et al. [36]	2020	NDN	Named based attacks (watchlist, sniffing attack), DDoS, time analysis attack, unauthorized access, traffic monitoring attack
Rao et al. [37]	2020	CCN	DoS attacks
Yong et al. [38]	2018	NDN	Watchlist, sniffing attacks, DoS, time analysis, caching pollution, bogus announcements attacks, jamming attack, time attack, flooding attack

4.3. Related Work on ICN-Based IoT with Machine Learning Technologies

Various research studies are reviewed concerning the ICN and the IoT with the classification of ML techniques and others. Next, the Results and Discussion are presented.

Gang et al. [39] proposed an enhanced distributed low-rate attack mitigating (eDLAM) mechanism that works on resisting new DoS attack types existing in the IoT. The paper established a game model as the first stage. This model analyzes the attack and helps to explain the benefit behind this attack between the attacker and the defender. Furthermore, the evaluation criteria of eDLAM's performance are in terms of the false negative rate and false positive rate. The paper mentioned that SDN is useful for separating control and forward functions to be applied to various IoT scenarios. In addition, this mechanism is implemented in the NDN architecture by NDN-Cxx and ndnSIM simulators.

Michael et al. [11] described a robust, efficient, and secure IoT network by analyzing the potential of the ICN. Then, they compared IP-based approaches with the ICN. They suggested using NDN to deploy the content-centric security model to resist DoS and enhance IoT industrial security. Furthermore, they suggested using the RIOT operating system for content security to deploy scenarios.

Tehseen et al. [40] reviewed IoT security issues, threats, and cyberattacks and presented an innovative method to protect all IoT devices by using ML and DL techniques. Moreover, this paper examined how ML and DL can be used to enhance attack detection and mitigation.

Kazeem et al. [9] reviewed methods used to detect and mitigate DDoS attacks on many Internet-enabled networks, including NDN, SDN, and IoT. In addition, it presented attack scenarios in some domains, such as the Internet of Drones, routing protocol-based IoT, and named-data networking. Furthermore, the paper observed that DDoS attacks are the most prevalent attack in the IoT, SDN, RPL-IoT, and NDN.

Haoyue et al. [10] presented a new mechanism to detect and mitigate one of the DoS attacks, called an IFA, by using ndnSIM simulation that realizes NDN and runs on an SDN-based platform.

A new app design called NDN4IoT was presented by [41], where the authors focused their design specifically on enhancing security and efficient analysis for the effectiveness of NDN-IoT devices. The FIWARE IoT platform is integrated with this app for some purposes, such as storing information about NDN-IoT devices and then making an analysis to decide whether the system or device fails. FIWARE is an open-source platform that provides APIs, a set of standards, and tools to develop IoT applications and enhance their security.

Azana et al. [42] presented the ICN as a solution for the IoT environment to enhance mobility and security. The network performance was evaluated based on general metrics, including service recovery time and packet loss cost.

Ravindran et al. [43] discussed ICN for the IoT in detail, including what the IoT requirements are, how ICN features will enhance the IoT environment, and what the challenges of an ICN-based IoT are.

Akhila et al. [44] proposed a strategy called UTS-LRU cache replacement that helps in evaluating the performance implications of one of the IoT network scenarios in the ICN. Then, the paper discussed the result that was defined by using the CCNx 1.0 protocol.

Sarika et al. [45] presented a network intrusion detection system (IDS) to be applied to the IoT. This paper focused on some attacks such as DoS and DDoS attacks using ML algorithms to detect all possible intrusions, such as deep neural network (DNN) and SVM. Finally, this paper only focused on the IoT.

Abdelhak et al. [8] introduced detection and mitigation mechanisms to identify malicious attacks in the NDN architecture by using an IDS. The paper discussed several attacks, such as DoS/DDoS, cache pollution attacks (CPAs), cache privacy attacks, cache poisoning attacks, and IFA. These attacks affect NDN operations. Furthermore, this paper presented the challenges and issues of NDN IDS in detail. Moreover, in one of the suggested models, the two main phases are the pre-attack phase and the main attack phase. In the pre-attack phase, the minimum re-transmission wait time, the minimum interest frequency, the topology characteristics, and the minimum number of pieces of content stored by malicious producers are identified. Accordingly, in the main attack phase, collecting the prefixes that are stored by the malicious producers is an important step, and then these malicious consumers set the interest frequency. The paper describes each attack mentioned in depth and how to mitigate them using IDS, but how to integrate NDN with the IoT and what potential issues and challenges there are were not mentioned.

Raneem et al. [46] proposed an approach that contains a multi-stage process for distinguishing intrusion activities from normal activities by using some techniques based on ML, such as k-means clustering that used the SLFN-SVM-SMOTE algorithm, and many others. The paper mentioned that the datasets CICIDS2017, UNSWNB15, and ISCX2012 are the most beneficial and well-known datasets. The NSL-KDD dataset is utilized to detect DoS attacks in the IoT environment. Furthermore, the most recent databases are LITNET-2020 and IoTD20; also, the BoT-IoT dataset is used in IoT environments. The paper discussed all these techniques and technologies for its proposed approach to mitigate attacks that pose a threat to the IoT system.

Sobia et al. [47] introduced the famous ICN architectures such as NDN that fit the requirements of IoT architectures with respect to their suitability in terms of caching, security, naming, and mobility handling schemes. In addition, they provided a classification of the ICN-based security scheme for IoT and mentioned that DoS may rise when the producer or intermediate routers set the freshness value for the required content. The paper reviewed ICN-IoT simulators and OSs, then discussed them; it identified the ndnSIM simulator as the most explored tool that goes well with implementing the IoT over the ICN. Then, issues, challenges, and future directions for the ICN in the IoT were discussed.

Ridha et al. [48] simply provided a review of ML algorithms and caching methods to integrate them with future network architectures such as SDN, ICN, NDN, 5G-ICN cellular networks, and edge computing.

Sedat et al. [21] provided a practical implementation of NDN-based IoT using the IfNoT mechanism to mitigate IFA. However, the paper mentions that in addition to their study, only one other study presents how to mitigate IFA in ICN-IoT. This proposed project was conducted using the ndnSIM simulator and the Contiki NG OS, which comes with the Cooja Network Simulator. The paper also reviewed other mitigation techniques and categorized them as statistical-based, collusive statistical-based, ML-based, and cryptography-based solutions. Regarding ML, the authors recommended several algorithms as the most effective ones in detecting and preventing IFA, including graph neural networks, RF, isolation forest, long short-term memory, and SVM. This is because ML algorithms differ from other traditional statistical approaches as they are adaptive and have a large capacity to detect attack patterns and prevent IFA from exposing the NDN-IoT networks. Table 4, presents a summary of ICN-based IoT threats and mitigation techniques.

Table 4. Summary of ICN-based IoT threats and mitigation techniques.

Author	Publication Year	Methodology	Technology	Threats and Challenges	Simulators and Datasets	Methods and Techniques	Limitations
Gang et al. [39]	2019	Quantitative	NDN-IoT integrated by SDN	DoS attacks	NDN-Cxx and ndnSIM simulations	eDLAM mechanism	ML technology is not mentioned
Michael et al. [11]	2018	Qualitative	NDN-IoT	DoS attack	CCN-Lite simulator	RIOT OS	ML technology is not mentioned
Tehseen et al. [40]	2023	Qualitative	IoT	Spoofing attacks, DoS, malicious code usage, data injection, MITM	Datasets such as NSL-KDD, UNSW-NB15, DARPA, CAIDA	DL, ML includes SVM, logistic regression, intrude tree, and behave DT	ICN including NDN is not mentioned
Kazeem et al. [9]	2023	Mixed	IoT NDN SDN RPL-IoT	DDoS attacks	Datasets such as NSL-KDD, DARPA'09 and KKD, drone data simulations	ML includes RF, DT, KNN, XGBoost, DT, J48, MLP + BP, SVM, and RF algorithms	No discussion of integrating IoT with NDN
Haoyue et al. [10]	2017	Mixed	NDN integrated with SDN	IFA	ndnSIM simulation	-	IoT technology and ML technology are not mentioned
Mohamed [41]	2023	Qualitative	NDN-IoT	-	NDN4IoT app	FIWARE platform	ML technology is not mentioned and no attack type is explored
Azana et al. [42]	2019	Qualitative	ICN-IoT	DoS	Simulators (NS-3, OMNeT, OPNET, GNS3, QualNet)	Wireshark	ML technology is not mentioned
Ravindran et al. [43]	2019	Qualitative	ICN-IoT	DoS, name spoofing attack, message manipulation attack, information modification attack	-	-	ML technology is not mentioned and no suggested simulator or dataset
Akhila et al. [44]	2016	Qualitative	ICN(CCN)-IoT	-	CCN-lite simulator	-	ML technology is not mentioned and no attack type is explored

Table 4. *Cont.*

Author	Publication Year	Methodology	Technology	Threats and Challenges	Simulators and Datasets	Methods and Techniques	Limitations
Sarika et al. [45]	2021	Qualitative	IoT	DoS, DDoS, replay attack, routing attacks	IDS KDD-Cup dataset	DNN, SVM, KNN, neural network, and random forest ML algorithms	ICN including NDN is not mentioned
Abdelhak et al. [8]	2022	Qualitative	NDN SDN	DoS, DDoS, cache pollution attacks, cache privacy attacks, cache poisoning attacks, and IFA	IDS	DNN, SVM, KNN, neural network, and random forest ML algorithms	IoT technology is not mentioned
Raneem et al. [46]	2021	Mixed	IoT	DoS, DDoS, and MITM	IDS datasets (CICID2017, UNSWNB15, ISCX2012, BoT-IoT, LITNET-2020, IoTD20)	SVM, SLFN-SVM-SMOTE, LR	ICN including NDN is not mentioned
Sobia et al. [47]	2018	Qualitative	ICN (NDN)-IoT	DoS	Simulations (CCN-lite, ndnSIM, NS-3, and Cooja) IoT OS (RRIOT OS, Contiki OS, FreeRTOS, OpenWSN, TinyOS)	-	ML technology is not mentioned
Ridha et al. [48]	2020	Qualitative	ICN-IoT SDN-NDN NDN ICN	-	-	ML type DQL (deep Q-learning), ILP (integer linear programming) ANN Deep RNN, RL, SNN	No attack type is explored and no suggested simulator or dataset
Sedat et al. [21]	2024	Mixed	NDN-IoT	IFA	ndnSIM simulation Contiki NG OS, Cooja	IfNoT mechanism	ML technology is mentioned as one of the solutions, but the proposed solution is built by the IfNoT mechanism

5. Results and Discussion

In the previous section, we reviewed comprehensive research papers about common cyberattacks in each ICN architecture: NetInf, NDN, DONA, CCN, PSIRP, and PURSUIT. The results showed that DoS attacks were the most executed attacks in all these architectures. On the NDN platform, while DoS attacks are prevalent, other attacks are also frequent, including watchlist sniffing, time analysis, caching pollution, bogus announcements, jamming, flooding, traffic monitoring, and passive and content poisoning. Some attacks do not happen traditionally; they are only applicable to ICN architectures. The other main architecture is CNN, which has features similar to NDN since they use the same hierarchical naming scheme. On the other hand, DONA, PSIRP, and PURSUIT use a flat naming scheme. DONA is the least prevalent and PSIRP faces attacks directly and indirectly because of hash content and hash from the publisher key. Moreover, NetInf is vulnerable to DoS/DDoS attacks. As a result, CCN and NDN are more frequently exposed and serve as rich platforms for DoS/DDoS attacks.

The most common cyberattacks are DoS, content poisoning, and cache pollution, which can be carried out on almost all architectures. According to our findings, as shown in Figure 8, first, NDN, the most common type, suffers 35% of the total attacks, such as DoS/DDoS attacks, watchlist sniffing attacks, and time analysis attacks. Second, CCN has 25% of the total attacks and DoS attacks are dominant. Third, DONA is the oldest platform, so many researchers avoid using it because more effective and secure architectures have been developed. Its percentage is only 15%. Finally, the results of PSIRP and PURSUIT, both posed attacks with only 10%. However, NetInf is in last place, with only 5%. According to recommendations, the architecture that should be used is NDN, which fits very well with the IoT because both are concerned with content.

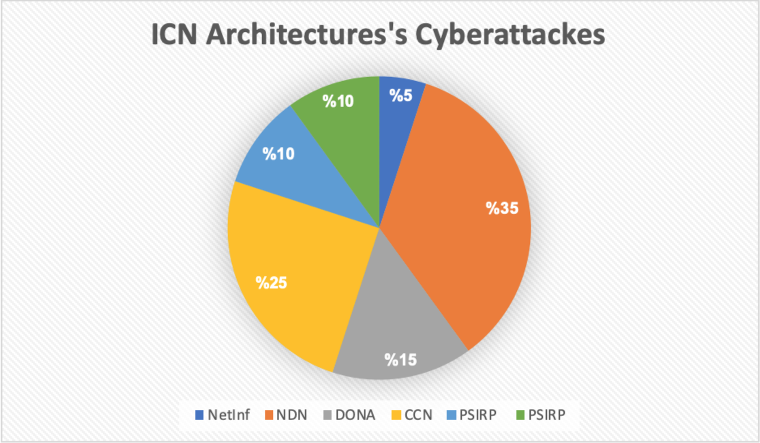

Figure 8. Cyberattacks on ICN architectures.

IoT three-layer architectures are a common way to structure IoT systems. The results of these IoT-related studies showed that there are common threats at each layer of IoT architecture. In the application layer, cloning attacks, eavesdropping, phishing attacks, malicious code injection, DoS attack, malicious viruses/worms/Trojan horses, and MITM attacks are considered the greatest threats because they pose a threat to the whole network.

Moreover, the main threats in the network layer include DoS/DDoS attacks, spoofing attacks, malicious code injection attacks, eavesdropping, sniffing attacks, and routing information attacks. Most of the analyzed studies focused on DoS/DDoS attacks and presented them as a major threat in this layer. DoS/DDoS attacks are easy to target and the first attack type that comes to the mind of attackers. They are attacks that aim to prevent authentic users from accessing devices or other network resources.

In the perception layer, some common threats are phishing attacks, malware attacks, DoS/DDoS, malicious script attacks, eavesdropping, node cloning, malicious code injection attacks, sniffing, spoofing, timing attacks, malicious node injection attacks, jamming attacks, and tag cloning. DoS/DDoS, malicious node injection attacks, and sniffing attacks are the major threats to the perception layer based on the analyses performed in these studies. Usually, attackers choose the easiest ways to gain access through devices and networks and attack the desired component. Figure 9 shows the most common threats based on application, network, and perception layers.

As a result, we deduce that the most dangerous cyberattacks are DoS/DDoS attacks, spoofing attacks, routing information attacks, and malicious code injection posing on the network layer. This is the reason why we worked on the network layer. Additionally, all layers share the following attacks: DoS/DDoS, malicious code injection, eavesdropping, and cloning attacks. As a result, these types of IoT-layer attacks were compared with the ICN architecture threats and the statistical results are shown in Figure 10.

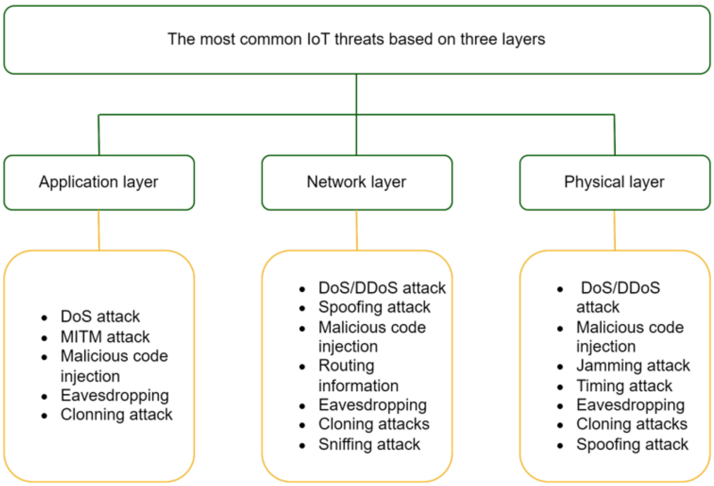

Figure 9. The most common IoT threats based on three layers.

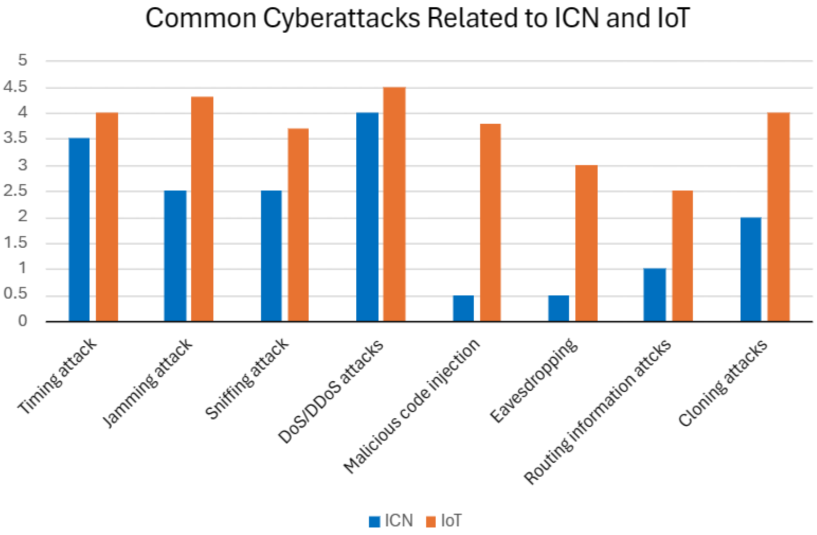

Figure 10. Common cyberattacks related to the ICN and the IoT.

According to the analyzed studies, the most common cyberattacks that have targeted ICN and IoT architectures are DoS and DDoS attacks. It was observed that DoS attacks pose significant challenges in both domains, emphasizing the necessity for finding effective solutions. Figure 10 categorizes these attacks based on the frequency of their mentions in the literature. For instance, the jamming attack is mentioned less frequently in ICN-related papers compared to IoT-related papers. However, DoS and DDoS attacks emerge as the most prevalent attack types in both the ICN and IoT domains.

As a result, the most common threats are DoS/DDoS attacks, and to detect and mitigate these types of attacks on ICN-based IoT, we must use one of the technologies such as artificial intelligence (AI), including DL and ML, edge computing, fog computing, and blockchain. There are also conventional solutions, but these are not recommended by researchers as technologies become very innovative. There are many algorithms that can be used with ML, such as RF, DT, KNN, XGBoost, DT, J48, MLP + BP, SVM, and RF. Using ML algorithms can be useful for anomaly detection in ICN-IoT networks. We select the SVM, RF, and KNN methods, as they go well with the ndnSIM simulator that we work with. Table 5 clarifies the purpose, advantages, and disadvantages of the selected ML methods, along with providing accuracy percentages to offer insights into the effectiveness of these methods. According to our findings, we work on the NDN architecture to enhance IoT networks by detecting and mitigating DoS attacks using ML technology. In addition, we recommend that researchers in this area focus on ML technologies.

Overall, ICN-IoT could be beneficial not only to the technical domain but also in various fields such as healthcare and smart homes. For safeguarding sensitive information in IoT applications, the ICN can be an effective solution due to its inherent data-centric approach, which provides better privacy protection. ICN networks can enhance security in various other domains such as supply chain management, finance, government, transportation, and utilities services fields. Furthermore, network administrators and policymakers should learn more about the benefits and challenges of adopting ICN-IoT technology to create appropriate strategies. For network administrators, this involves adapting to the specific characteristics of ICN-IoT networks, including understanding routing and caching mechanisms and how to analyze this type of network. However, policymakers may need to establish new guidelines for data privacy and security when using ICN-IoT.

Table 5. Comparison between SVM, KNN, and RF ML algorithms.

ML Technique	Purpose	Advantages	Disadvantages	Accuracy Percentage
SVM	• To classify various attack types • Features selection and intrusion detection	• Robust in high-dimensional spaces • Powerful algorithm	• May require significant memory resources, particularly in scenarios with a high number of features • Ineffective for datasets with a large number of rows	• 99.4%
KNN	• Network IDS • To reduce the false alarm rate	• Simple implementation	• Long prediction time	• 98.35%
RF	• To build network IDS	• More robust and accurate predictions	• Complexity may affect the training time of the model	• 99.98% better than SVM and KNN

6. Recommendations and Future Research Directions

The previous papers contained most of the information we needed to present our paper. The most used ICN architecture, known as NDN, is suitable for integrating with the IoT. NDN can easily operate above the network layer as many simulators allow us to experiment with an NDN-based IoT immediately. In addition, there are many DoS attack types that were included and discussed in the previous papers and some of them take place only when the two architectures are integrated, such as in the IFA.

The reviewed literature showed that high numbers of ML algorithms have been experimented with on either IoT, one of the ICN architectures, or in SDN. However, in the case of integrated NDN with the IoT, there are few studies and no implementation of ML algorithms. On the other hand, no article explains or applies how can we mitigate and prevent DoS attacks by using ML technology for ICN-IoT networks. Accordingly, no dataset is right for us, and most of the papers that worked with the ICN deal with simulators. We summarize the following future directions of ICN-IoT security:

- We recommend more future research investigations to enhance ICN-IoT security.
- We recommend more future research investigations concerning ICN-IoT implementation in the security field.
- We recommend more future research investigations into the use of ML technology to improve the security of ICN-IoT.
- We recommend more future research investigations to test and train a variety of ML classifiers to identify the most effective option used to improve the security of the ICN-IoT network.
- We recommend more future research investigations to explore other attack types and threats on the ICN-IoT.
- We recommend more future research investigations to expand the implementation process by using DL technology after the initial results of ML classifiers by training various DL classifier types to increase the security level of ICN-based IoT.

- We recommend more future research investigations using other technologies such as DL, fog computing, and blockchain to compare the results between them and identify which one provides the most effective results to improve the security of ICN-IoT against cybersecurity attacks.

7. Conclusions

In conclusion, this paper discusses ICN architectures and how the ICN integrates with the IoT. The paper provides a comprehensive literature review, including common cybersecurity threats, with particular emphasis on DoS attacks. The analysis highlights that DoS attacks pose a significant challenge to both the ICN and IoT, so we present some detecting and mitigating techniques through integrated ML technologies, such as SVM, RF, and KNN to enhance security measures against these attacks. Further investigations are discussed and emphasize ML-based approaches for ICN-IoT security. The new proposed approach is based on the NDN architecture that relies on the ndnSIM simulator, which is considered an IDS, to prevent DoS attacks from exposing IoT devices. Overall, future studies should expand their research, explore additional attack types and threats on the ICN-IoT, and enhance security using ML technology by advancing innovative solutions for robust and resilient network architectures.

Author Contributions: Conceptualization, R.B. and A.A.; methodology, R.B., A.A. and M.M.H.R.; software, R.B. and A.A.; validation, R.B., A.A. and M.M.H.R.; formal analysis, R.B., A.A. and M.M.H.R.; investigation, R.B. and A.A.; resources, R.B. and A.A.; writing—original draft preparation, R.B.; writing—review and editing, R.B. and A.A.; supervision, A.A. and M.M.H.R.; project administration, A.A. and M.M.H.R.; funding acquisition, A.A. and M.M.H.R. All authors have read and agreed to the published version of the manuscript.

Funding: This paper was funded by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [GRANT 5933].

Data Availability Statement: Data available in a publicly accessible repository.

Acknowledgments: The authors would like to thank the anonymous reviewers for their insightful scholastic comments, directions and suggestions, which improved the quality of the paper.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
ICN	Information center network
IFA	Interest flooding attack
ML	Machine learning
DoS	Denial-of-service attack
DDoS	Distributed denial-of-service
IP	Internet Protocol
TCP	Transmission Control Protocol
AI	Artificial intelligence
NDN	Named-Data Networking
CCN	Content-Centric Networking
PSIRP	Publish–Subscribe Internet Routing Paradigm
DONA	Data-Oriented Network Architecture
NetInf	Network of information
SVM	Support vector machine
KNN	K-nearest neighbor
RF	Random forest
MITM	Man-in-the-middle
PURSUIT	Publish–Subscribe Internet Technology

SAIL	Scalable & Adaptive Internet Solutions
COMET	Content Mediator Architecture for Content-Aware Networks
4WARD	Architecture and Design for the Future Internet
CR	Content router
CS	Content store
FIB	Forwarding information base
PIT	Pending interest table
IFA	Interest flooding attack
BIFA	Basic IFA
CIFA	Collusive IFA
SCAN	Smart collaborative attack in NDN
NRS	Name-resolution system
IoV	Internet of Vulnerabilities
IIoT	Industrial Internet of Things
SDPC	Secure distribution of protected content
eDLAM	Enhanced distributed low-rate attack mitigating
DL	Deep learning
IDS	Intrusion detection system
DNN	Deep neural network
CPA	Cache pollution attacks
WSN	Wireless sensor network
WBAN	Wireless body area network
JS	Jensen–Shannon
DT	Decision tree
MLP	Multilayer perceptron
BP	Backpropagation
SDPC	Secure distribution of protected content

References

1. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet Things* **2020**, *11*, 100227. [CrossRef]
2. Mishra, S.; Jain, V.K.; Gyoda, K.; Jain, S. An efficient content replacement policy to retain essential content in information-centric networking based internet of things network. *Ad Hoc Netw.* **2024**, *155*, 103389. [CrossRef]
3. Rahman, A.; Hasan, K.; Kundu, D.; Islam, M.J.; Debnath, T.; Band, S.S.; Kumar, N. On the ICN-IoT with federated learning integration of communication: Concepts, security-privacy issues, applications, and future perspectives. *Future Gener. Comput. Syst.* **2023**, *138*, 61–88. [CrossRef]
4. Krishna, B.V.S.; Gnanasekaran, T. A systematic study of security issues in Internet-of-Things (IoT). In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017; pp. 107–111. [CrossRef]
5. Sadhu, P.K.; Yanambaka, V.P.; Abdelgawad, A. Internet of Things: Security and Solutions Survey. *Sensors* **2022**, *22*, 7433. [CrossRef] [PubMed]
6. Nour, B.; Mastorakis, S.; Ullah, R.; Stergiou, N. Information-Centric Networking in Wireless Environments: Security Risks and Challenges. *IEEE Wirel. Commun.* **2021**, *28*, 121–127. [CrossRef]
7. Tourani, R.; Misra, S.; Mick, T.; Panwar, G. Security, Privacy, and Access Control in Information-Centric Networking: A Survey. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 566–600. [CrossRef]
8. Hidouri, A.; Hajlaoui, N.; Touati, H.; Hadded, M.; Muhlethaler, P. A Survey on Security Attacks and Intrusion Detection Mechanisms in Named Data Networking. *Computers* **2022**, *11*, 186. [CrossRef]
9. Adedeji, K.B.; Abu-Mahfouz, A.M.; Kurien, A.M. DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges. *J. Sens. Actuator Netw.* **2023**, *12*, 51. [CrossRef]
10. Xue, H.; Li, Y.; Rahmani, R.; Kanter, T.; Que, X. A mechanism for mitigating DoS attack in ICN-based internet of things. In Proceedings of the Proceedings of the 1st International Conference on Internet of Things and Machine Learning, New York, NY, USA, 17–18 October 2017. [CrossRef]
11. Frey, M.; Gündoğan, C.; Kietzmann, P.; Lenders, M.; Petersen, H.; Schmidt, T.C.; Juraschek, F.; Wählisch, M. Security for the Industrial IoT: The Case for Information-Centric Networking. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; pp. 424–429. [CrossRef]
12. Amadeo, M.; Campolo, C.; Quevedo, J.; Corujo, D.; Molinaro, A.; Iera, A.; Aguiar, R.L.; Vasilakos, A.V. Information-centric networking for the internet of things: Challenges and opportunities. *IEEE Netw.* **2016**, *30*, 92–100. [CrossRef]
13. Nour, B.; Sharif, K.; Li, F.; Biswas, S.; Moungla, H.; Guizani, M.; Wang, Y. A survey of Internet of Things communication using ICN: A use case perspective. *Comput. Commun.* **2019**, *142–143*, 95–123. [CrossRef]

14. Ahmed, S.F.; Shuravi, S.; Bhuyian, A.; Afrin, S.; Mehjabin, A.; Kuldeep, S.A.; Alam, M.S.B.; Gandomi, A.H. Navigating the IoT landscape: Unraveling forensics, security issues, applications, research challenges, and future. *arXiv* **2023**, arXiv:cs.NI/2309.02707.
15. Obaidat, M.A.; Obeidat, S.; Holst, J.; Al Hayajneh, A.; Brown, J. A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. *Computers* **2020**, *9*, 44. [CrossRef]
16. Yoachimik, O.; Pacheco, J. *DDoS Threat Report for 2023 Q4*; Cloudflare: San Francisco, CA, USA , 2024. Available online: https://blog.cloudflare.com/ddos-threat-report-2023-q4 (accessed on 28 January 2024).
17. Wang, J.; Jiang, C.; Zhang, H.; Ren, Y.; Chen, K.C.; Hanzo, L. Thirty Years of Machine Learning: The Road to Pareto-Optimal Wireless Networks. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1472–1514. [CrossRef]
18. Dalmazo, B.L.; Marques, J.A.; Costa, L.R.; Bonfim, M.S.; Carvalho, R.N.; da Silva, A.S.; Fernandes, S.; Bordim, J.L.; Alchieri, E.; Schaeffer-Filho, A.; et al. A systematic review on distributed denial of service attack defense mechanisms in programmable networks. *Int. J. Netw. Manag.* **2021**, *31*, e2163. [CrossRef]
19. Srinivasan, K.; Mubarakali, A.; Alqahtani, A.S.; Dinesh Kumar, A. A Survey on the Impact of DDoS Attacks in Cloud Computing: Prevention, Detection and Mitigation Techniques. In *Intelligent Communication Technologies and Virtual Mobile Networks*; Balaji, S., Rocha, Á., Chung, Y.N., Eds.; Springer: Cham, Switzerland, 2020; pp. 252–270.
20. AbdAllah, E.G.; Hassanein, H.S.; Zulkernine, M. A Survey of Security Attacks in Information-Centric Networking. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1441–1454. [CrossRef]
21. Bilgili, S.; Demir, A.K.; Alam, S. IfNot: An approach towards mitigating interest flooding attacks in Named Data Networking of Things. *Internet Things* **2024**, *25*, 101076. [CrossRef]
22. Alashhab, A.A.; Zahid, M.S.M.; Azim, M.A.; Daha, M.Y.; Isyaku, B.; Ali, S. A Survey of Low Rate DDoS Detection Techniques Based on Machine Learning in Software-Defined Networks. *Symmetry* **2022**, *14*, 1563. [CrossRef]
23. Altulaihan, E.; Almaiah, M.A.; Aljughaiman, A. Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms. *Sensors* **2024**, *24*, 713. [CrossRef]
24. Aslam, M.; Ye, D.; Tariq, A.; Asad, M.; Hanif, M.; Ndzi, D.; Chelloug, S.A.; Elaziz, M.A.; Al-Qaness, M.A.A.; et al. Adaptive Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation System for SDN-Enabled IoT. *Sensors* **2022**, *22*, 2697. [CrossRef] [PubMed]
25. Kumar, N.; Singh, A.K.; Srivastava, S. Evaluating machine learning algorithms for detection of interest flooding attack in named data networking. In Proceedings of the 10th International Conference on Security of Information and Networks, New York, NY, USA, 13–15 October 2017; pp. 299–302. [CrossRef]
26. Alabsi, B.A.; Anbar, M.; Rihan, S.D.A. Conditional Tabular Generative Adversarial Based Intrusion Detection System for Detecting Ddos and Dos Attacks on the Internet of Things Networks. *Sensors* **2023**, *23*, 5644. [CrossRef] [PubMed]
27. Deep, S.; Zheng, X.; Jolfaei, A.; Yu, D.; Ostovari, P.; Kashif Bashir, A. A survey of security and privacy issues in the Internet of Things from the layered context. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e3935. [CrossRef]
28. Albalawi, A.M.; Almaiah, M. Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in IoT environment. *J. Theor. Appl. Inf. Technol.* **2022**, *100*, 2988–3011.
29. Iqbal, W.; Abbas, H.; Daneshmand, M.; Rauf, B.; Bangash, Y.A. An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security. *IEEE Internet Things J.* **2020**, *7*, 10250–10276. [CrossRef]
30. Jayasinghe, K.; Thalawattha, S.; Rodrigo, R.; Dissanayaka, D.; Kathriarachchi, R. A Defence Against an Internet of Things (IoT) Attacks Based on Current Vulnerabilities. In Proceedings of the International Conference on Advancement of Development Administration, Bangkok, Thailand, 28–30 May 2020.
31. Alferidah, D.K.; Jhanjhi, N.Z. A Review on Security and Privacy Issues and Challenges in Internet of Things. *Int. J. Comput. Sci. Netw. Secur.* **2020**, *20*, 263–286.
32. Burhan, M.; Rehman, R.A.; Khan, B.; Kim, B.S. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors* **2018**, *18*, 2796. [CrossRef] [PubMed]
33. Verma, G.; Prakash, S. Emerging Security Threats, Countermeasures, Issues, and Future Aspects on the Internet of Things (IoT): A Systematic Literature Review. In *Advances in Interdisciplinary Engineering*; Kumar, N., Tibor, S., Sindhwani, R., Lee, J., Srivastava, P., Eds.; Springer: Singapore, 2021; pp. 59–66.
34. Pal, S.; Jadidi, Z. Analysis of Security Issues and Countermeasures for the Industrial Internet of Things. *Appl. Sci.* **2021**, *11*, 9393. [CrossRef]
35. Ahlgren, B.; Dannewitz, C.; Imbrenda, C.; Kutscher, D.; Ohlman, B. A survey of information-centric networking. *IEEE Commun. Mag.* **2012**, *50*, 26–36. [CrossRef]
36. Bilal, M.; Pack, S. Secure Distribution of Protected Content in Information-Centric Networking. *IEEE Syst. J.* **2020**, *14*, 1921–1932. [CrossRef]
37. Rais, R.N.B.; Khalid, O. Study and analysis of mobility, security, and caching issues in CCN. *Int. J. Electr. Comput. Eng. (IJECE)* **2020**, *10*, 1438–1453. [CrossRef]
38. Yu, Y.; Li, Y.; Du, X.; Chen, R.; Yang, B. Content Protection in Named Data Networking: Challenges and Potential Solutions. *IEEE Commun. Mag.* **2018**, *56*, 82–87. [CrossRef]
39. Liu, G.; Quan, W.; Cheng, N.; Zhang, H.; Yu, S. Efficient DDoS attacks mitigation for stateful forwarding in Internet of Things. *J. Netw. Comput. Appl.* **2019**, *130*, 1–13. [CrossRef]

40. Mazhar, T.; Talpur, D.B.; Shloul, T.A.; Ghadi, Y.Y.; Haq, I.; Ullah, I.; Ouahada, K.; Hamam, H. Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence. *Brain Sci.* **2023**, *13*, 683. [CrossRef] [PubMed]
41. Hail, M.A.M. Efficient Management, Control and Analysis of IoT-NDN Devices through "NDN4IoT" App Integrated with FIWARE. In Proceedings of the 2023 12th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 6–10 June 2023; pp. 1–4. [CrossRef]
42. Aman1, A.H.M.; Hassan, R. Internet Protocol Function Enhancement using Information Centric Approach to Solve Mobility and Security Problems for Internets of Things. In Proceedings of the 1st International Conference on Informatics, Engineering, Science and Technology, INCITEST 2019, Bandung, Indonesia, 18 July 2019. [CrossRef]
43. Ravindran, R.; Zhang, Y.; Grieco, L.A.; Lindgren, A.; Burke, J.; Ahlgren, B.; Azgin, A. Design Considerations for Applying ICN to IoT. In *Internet-Draft Draft-Irtf-Icnrg-Icniot-03, Internet Engineering Task Force*; Work in Progress; 2019. Available online: https://datatracker.ietf.org/doc/draft-irtf-icnrg-icniot/ (accessed on 28 January 2024).
44. Rao, A.; Schelén, O.; Lindgren, A. Performance implications for IoT over information centric networks. In Proceedings of the Eleventh ACM Workshop on Challenged Networks, New York, NY, USA, 3–7 October 2016; pp. 57–62. [CrossRef]
45. Choudhary, S.; Kesswani, N.; Majhi, S. An Ensemble Intrusion Detection Model For Internet of Things Network. *Res. Sq.* 2021, *preprint*. [CrossRef]
46. Qaddoura, R.; Al-Zoubi, A.M.; Almomani, I.; Faris, H. A Multi-Stage Classification Approach for IoT Intrusion Detection Based on Clustering with Oversampling. *Appl. Sci.* **2021**, *11*, 3022. [CrossRef]
47. Arshad, S.; Azam, M.A.; Rehmani, M.H.; Loo, J. Recent Advances in Information-Centric Networking-Based Internet of Things (ICN-IoT). *IEEE Internet Things J.* **2019**, *6*, 2128–2158. [CrossRef]
48. Negara, R.M.; Rachmana Syambas, N. Caching and Machine Learning Integration Methods on Named Data Network: A Survey. In Proceedings of the 2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA), Bandung, Indonesia, 4–5 November 2020; pp. 1–6. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.