A Comprehensive Exploration of Storage Attacks inInformation-Centric Networking Environments

Sethu S
Department of Computer Science and Engineering
Vels Institute of Science, Technology & Advanced Studie
Tamil Nadu, India.
Sethu.se@velsuniv.ac.in

Manikandan A
Department of Computer Science and Engineering
Vels Institute of Science, Technology & Advanced Studies
Tamil Nadu, India.
mani.se@velsuniv.ac.in

Abstract—To help users overcome the limitations of current IP networks, Data Networking (NDN) and Content-Centric Network (CCN) architectures have been created to move communication from host-centric to content-centric. NDN is essentially a network for the dissemination of content. In NDN, a user's request for material will be the only reason for contact. The descriptive capabilities of NDN technology leverage the globally unique names that encryption and content-based security provide. As part of its design, it upholds content validity and reliability. We examine several storage risks that NDN caches face, including content poisoning attacks, cache pollution attacks, and man-in-the-middle attacks.

Keywords—Host-centric communication paradigm, Intra-network caching Technology, Content Centric network, Prefix hijacking and black holing, Token bucket with interface specific parity, Collaborative signature verification, Transmission Control, Interest packets, Data packets.

I. Introduction

A novel networking paradigm known as information-centric networking presents a host-centric communication paradigm that identifies and routes traffic using IP addresses and TCP/UDP ports and is being replaced by ICN. ICN uses content names, which represent the data itself, to enable communication between nodes in the network rather than host-centric IDs. Host-centric communication models give way to content-centric ones in the NDN, which are driven by consumers.

NDN mostly possesses the following traits:

- By prioritizing named content above IP addresses and employing content-based routing names, one may concentrate on the content itself rather than its location.
- NDN introduced intra-network caching technology, which allows the content to be answered from several locations and the router to store it.
- The receiving end implements transmission control, and the receiver-driven method of transmission is designed. [1].

An overview of NDN and its fundamental ideas is given in this study, which also discusses various attack types such interest flooding, man-in-the-middle, content poisoning, and cache pollution, and suggests strategies to improve cache dependability and efficacy. As a result, by improving data transport and decreasing retrieval latency. The remainder of the work is structured as follows. Section II provides a quick overview of the NDN architecture. Section III describes the related study on this topic. Many attack types and their defenses are covered in Section IV, and future research is

II. NDN ArchitectureNDN Architecture

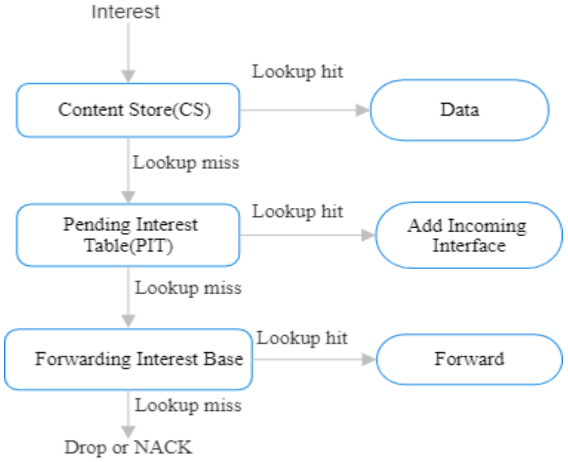

Fig 1. Forwarding Process in NDN

Fig 1.Show in Forwarding Process in NDN NDN is used to name data bits to connect computing devices, from Internet of Things sensors to cloud servers. When a user requests data in NDN, the data is given a distinct name (which is similar to a URL) that is used to retrieve the data. When the user requires data, the request is transmitted to the network. Every router on the network that has a duplicate of the data request responds with the data. The user can get the data from the nearest router. This means that you don't need a specific source of data, and you can get the data faster[13].

NDN router Consists of three tables namely

A. Content Store (CS).
B. Table of Pending Interests (PIT)
C. Information Base for Forwarding (FIB)

A. The Content Store

The data structure like the content store is used to store and manage content in NDN routers. It serves as a temporary cache for frequently needed data, enabling quicker retrieval of information and decreasing the need for repeated data exchanges. In NDN, when a data request is made, the router checks its content store table whether an exact copy of that data is available, if it is available it is provided to the requester immediately, eliminating the

979-8-3503-8434-5/24/$31.00©2024 IEEE

requirement to retrieve it from the source [23]. This is known as in-network caching, and it is a critical element of NDN. As new data is requested, the content store table is regularly updated, and old data is evicted to create a place.

B. Table of Pending Interests (PIT)

Tracking pending interests in NDN is done by a data structure called the Table of Pending Interest, or Pending Interest Table. An interest packet sent by a customer for a a particular piece of information is kept in the PIT until the item is found and delivered. The PIT is simply a cache that retains the interests for a specified interval of time, which enables successful retrieval methods that result in processing the full stuff without focusing on a specific species and creating unwanted data during processing [7].

C. Forwarding Information Base (FIB)

It stores the routing information necessary for data delivery. It contains a list of content names and the interfaces to which the router utilizes to forward data packets. When a data request arrives, the router consults the FIB to find the optimum information transmission path [1]. This is known as name-based forwarding, and it is an important component of content-centric networking. Fig 2 Show in NDN types of packets.

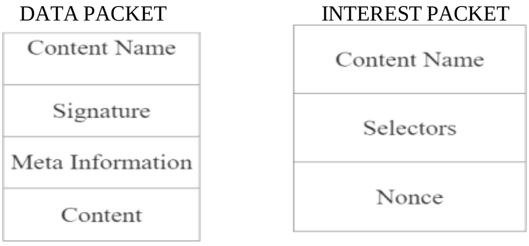

Fig 2. NDN types of packets

NDN, a customer-driven model, the customer begins sending interest packets to the router, and the router replies with data packets if they contain specific data; otherwise, they are placed in the Pending Interest Table (PIT) [6]

III. RELATED WORK

This section examines numerous research articles on NDN architecture, security, and various sorts of attacks.

The fundamental ideas, properties, functions, and operations of NDN [13] are described. Paolo Gasti et al. suggest numerous denials of service (DOS) and distributed denial of service (DDOS) attacks, along with new forms of attacks and defences [16].

Mauro Conti and colleagues concentrate on buffer contamination assaults, wherein the adversary manipulates cache locations to escalate link utilization and cause cache misses for truthful users. Through simulations, we demonstrate that these kinds of attacks are feasible in NDN with few resources and that they also work well in larger topologies. [12].

Lin Yao et al. described in [15] a clustering method (content interest) for identifying buffer poisoning attacks and defending against them using ZIPF-like distribution by updating the table with atypical requests to inform the nodes. In this case, ndnSIM is employed to successfully resist the CPA.

Lin Yao et al. identify and defend against storage poisoning attacks using popularity prediction in NDN in [18]. The main defense tactic will be to prevent the spread of suspicious content once it has been established that the attack lessens the impact of the pollution attack with a higher cache hit, a higher detection ratio, and a lower hop count in comparison to other state-of-the-art methods.

Defenses against replay attacks, man-in-the-middle attacks (MITM), and content poisoning attacks (CPA) were among the three types of attacks that Mohammed et al. discussed in [6]. Cache pollution attack types, detection techniques, countermeasure calculation, and memory consumption are all covered. PPKD or signature verification is the basis for the content poisoning attack detection type, as Naveenkumar et al. explains in [23].

Using ndnSim simulations, Abdelhak et al. [3] analyzed the CPA, one of these attacks that is most successful, and assessed its influence on NDN. A variety of situations in simple, clever, and real topologies were used to illustrate how a CPA affects cache efficiency. These studies show that a CPA can have highly negative effects, such as lowering the HDR to 0.6, raising the ARD to around 20%, and lowering the CHR to about 0% in some circumstances.

Hanai Salah et al. describe CoMon++, a useful defense against buffer poisoning threats in NDN, in this study [22]. Guanglin Xing et al. claim that planned IFAs may result in major network safety flaws that need to be fixed. An IFDM method for handling IFAs is proposed in this paper. The proposed method computes a variance value on every prefixed value using an iForest to identify problematic prefixes. The goal of this rate limitation is to lower IFA by preventing rogue data from entering the network. In summary, simulation findings show that the IFDM technique effectively enhances assault and decreases incorrect conclusions brought on by packet destruction during PIT overflow[8].

Gergely Acs et al. described several solutions for balancing privacy and latency in [20]. These tactics were analyzed in terms of both nearby and remote adversaries, and an official framework that enables us to measure the privacy state provided by various storage strategies is also described.

IV. SECURITY ATTACKS

In this section, the various security attacks are concentrated and their measures are also discussed in detail in each section. Fig 3Show in Various Types of Attacks.

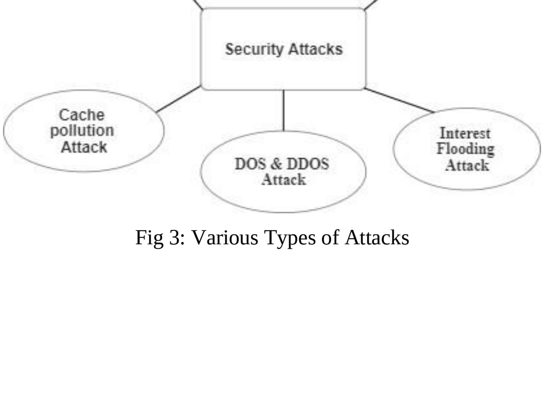

Fig 3: Various Types of Attacks

A. Man In The Middle Attack (MITM):

NDN data-centric security must achieve three primary goals. They are

1) Data Integrity: It asserts that information cannot bechanged once it has been created.

2) Data Authenticity: It asserts that the purported producer of the data produces it.

3) Access Control: This specifies that information shall only be retrieved and published by consumers (producers) who have the necessary authorization.

Public-key cryptography has been directly used by the NDN to achieve these goals. Among the attacks on reliability is an attack known as Man-in-the-Middle (MITM) [6]. It is performed by employing hostile nodes or outsiders to capture and seize command of the medium of communication between two nodes, which are typically the router and the terminal user. Although MITM has been around for a long, denial-of-service attacks in the NDN architecture are more common. The main ability of MITM is to surreptitiously take control using transmission link packet intercepts. MITM can merge several or additional data packets under one name within an NDN network but with separate content and a different signing key. MITM can operate at several OSI (Open Systems Interconnection) architectural layers to undermine content integrity. MITM attacks can be categorized into two types.

a) Passive MITM: An attacker focuses on user-to-packet tracking, whereas passive MITM attempts to identify the material being exchanged.

b) Active MITM: The victim-to-victim interaction will be watched, noted, and captured by the attacker. A content breach leads to the loss of content integrity. Serious injuries are sustained by active MITM victims [6].

B. Countermeasure Technique for the MITM Attack:

a) Name-Based Access Control: Access control that is based on encryption is one method for verifying the authenticity and consistency of the information. Name-based security for ICN (NBS-ICN), as proposed by the authors of [6], ensures content integrity through the use of decentralized identifiers, identity-based intermediary second encryption, and identity-based cryptography. The owner's digital signature protects integrity and makes it possible to certify the content's legitimacy. By using a simple challenge-response mechanism for user authentication, MITM attacks can be prevented. The customer needs to answer by digitally signing a random number generated by the register. All TLS messages follow this protocol.

b) Identity-Based Access Control : Using identity-based proxy re-encryption, this approach protects information from providers of content in Publisher Subscriber Internet PSI-ICN. Their access control methods will encrypt the stuff on their own. Two identifiers are used to identify the content (Sid): the location of the meeting identifier (RId) and the range identifier. RIds are unique within a scope, whereas SIds are unique globally. By providing a "clue" about the network that contains an information product, SIDS are utilized. Every Sid is controlled specifically by an identification node known as the reunion node (RN), where "SId" is kept.

C. Content Poisoning Attack:

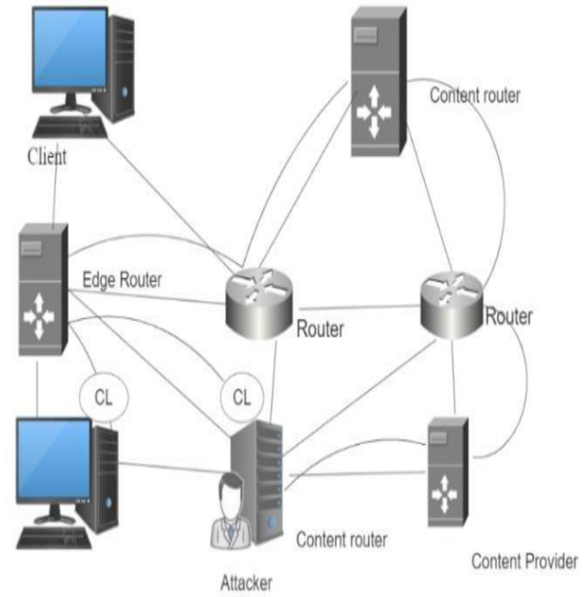

Fig 4 : Content Poisoning Attack

Fig 4 .Show in Content Poisoning Attack When a router is infiltrated, it may show manipulated or fraudulent content in response to a material request. The other routers involved in the transmission save this information in their CS. As more authorized users looked for them, the contaminated contents spread [23]. The content poisoning attack aims to introduce false information into router caches. An attacker has to take control of one or more intermediate routers to introduce its content into the network. The inserted material contains a false payload or an incorrect signature, but its name is legitimate and matches an interest. to the digest and remove packets whose hashes don't match, even whether they have a fake payload or an invalid signature. This attack applies to all ICN ideas, but it performs less well in systems that rely on self-certifying names. A self-certifying packet's name is its content hashed together. As such, it is easier to verify the validity of a content chunk by comparing its hash to the digest and removing packets whose hash does not match.[11].

Fig 4 depicts the poisoning attack. As one of the routers bridging the gap between the client and the provider. An attacker might flood the network with malicious content objects if the material is not verified, making it impossible for valuable data to reside in the caches. This attack could be extremely damaging.

D. Countermeasure Technique for Content Poisoning Attacks

There are two methods for dealing with Content Poisoning Attacks. The consumer is responsible for collaborative signature verification. Networks, where routers cooperate to verify the content signature, are known as collaborative signature verification systems.

Client feedback or additional fields in requests and data packets are used by consumer-dependent approaches.

a) Collaborative Signature Verification

Methods that suggest router verification of packet signatures before packet forwarding fall into this category. To spread and reduce the load of signature authentication, networks can either label the authenticated fragments to alert other devices that the packet has been validated or verify the chunks' identities on cache hit (validating only popular material). The content-poisoning attacks were initially addressed by Reza et al. [11]. As an initial countermeasure, the authors suggested helping routers validate incoming information chunks by employing a "self-certifying interest/data packet" (SCID).

A client must obtain from the content provider the hash, name, and signature of the required chunk before submitting an interest. The interest is connected to this data. By verifying the encrypted version of a content chunk it receives to the hash of the interest data that previously produces, a router can confirm the legitimacy of the content chunk. Although this method uses less computing power than conventional signature validation, it still results in higher content retrieval latency, higher router storage overhead, and less scalability because the end user is required to collect hash codes for each packet or data chunk ahead of time, which the routers then need to store until authentication. Routers verify the signature of cached material as an added feature. In the most basic configuration, every router selects and verifies information blocks by arbitrarily discarding those whose signatures are unverifiable. Routers select a group of information blocks to verify collectively to prevent repeated verification. The extent of this connection may differ from community to neighborhood. However, the strategy carries disadvantages. When a chunk is asked for twice and requires to be checked and confirmed, there is an increase in processor delay and processing time. An attacker can force it by persistently demanding authentication of all fake material; on a large-scale, this could lead to a DoS/DDoS assault

b) Consumer Dependency

A. Clients might offer input regarding the authenticity of the content they have received or supply public keys to the providers in their request packets to facilitate verification in consumer-dependent countermeasures. An approach for avoiding content contamination while offering a revised definition of false content. The authors characterized false content as having a valid signature but utilizing the incorrect key or having an incorrect identity field. The paper's authors covered well-known fixes, such as the impossibility of line-speed signature verification using intermediary routers. Conversely, self-certifying names is a more effective countermeasure; nonetheless, issues like managing dynamic content objects and efficiently retrieving content hashes still need to be addressed. Consequently, a feedback-based, exclusion-based ranking system for cached information has been created.

E. Cache Pollution Attack:

Cache Pollution Attacks (CPA) aim to reduce the volume of cache available in the Content Store (CS) while preventing other genuine consumers from accessing the cache. The attackers begin requesting renowned information from a fake source, who complies. These papers save information store spaces for subsequent queries, and they repeatedly retrieve identical content, making full use of the cache's capacity and converting this unwanted content to highly valued items that stay in the database for extended periods. As a result, they complicate the caching decisions, resulting in a reduction in store success frequency for the designated routers and a hike in the retrieval of information delay for genuine users. Because it alters the data provided from the temporary storage and takes an unpredictable amount of time to complete, this sort of assault is relatively easy to execute but difficult to identify. In certain situations, this exceeds the router's capacity and depletes a significant amount of the Content Store (CS) resources.

F. Countermeasure Technique for Cache Pollution Attack:

a) Trial-and-error: The basis of reinforcement learning interactions between the agent and the surroundings, as well as continual behavior modification based on environmental information, is trial-and-error learning. The application examines the condition of the surrounding Qt at each interval t. The newly formed state Qt+1 and the associated reward Rt are acquired when the player acts while in the Qt state.

Their goal is to increase the payout Gt. The reduction factor, denoted by, has a range of [0,1]. The reward function, state, action, and transition probability are the four fundamental components of reinforcement learning. DRL is a synthesis of reinforcement learning decision-making with deep learning perception. Its great generality enables it to directly regulate from beginning input to output via end-to-end learning. Reinforcement learning decision-making in a generalized form is combined with deep learnin g perception to create DRL At each moment of interaction with the outside world, an agent's acquisition of knowledge begins when it learns an observation of the surroundings, also known as the state. The incredibly complicated state is reduced to the low-dimensional features using deep learning techniques. At every stage, the agent will receive recognition for their actions. At every stage, the agent needs to optimize the whole advantage. The aggregate estimated value that can be acquired by acting at the state level is represented by the value function Q(st, at) at the state level. Finding the best value function is the agent's responsibility. After making a decision, it modifies the condition of the environment and collects the subsequent observation.

G. Dos and DDos Attack:

Attacks known as denial of service (DoS) and distributed denial of service (DDoS) are growing in popularity. When a server is overloaded with traffic, a DoS attack, which stands for denial-of-service prevents an internet page or another server from operating. Distributed denial-of-service (DDoS) attacks are one type of DoS attack that involves flooding a particular resource with traffic from numerous computers or terminals. DDoS attacks have recently emerged as the most vexing and time-consuming issue. Attacks are becoming more common and involving greater amounts of data—

hundreds of terabytes rather than merely gigabytes. Detecting these attacks effectively is difficult due to differences in attack patterns or novel modes of attack[24]. Numerous host and network resources, protocol tiers, and particular applications are the targets of a broad range of denial-of-service attacks. An attack typically consists of three components: Three things can happen: (1) a group of zombies controlled by one or more master nodes; a group of victim hosts and/or routers; and (3) a master node or master nodes.

a) Attacks by Reflection: A reflection assault involves three entities: the opponent, the one being attacked host, and several additional attackers known as reflectors Using the reflectors, the opposing party intends to swamp the intended host with traffic. In a faked IP packet, the attacker swaps the address of its aimed target using its own, sends the messages to the secondary victims, and executes an indirect hit. The responses overburden the target instead of routing them back to the enemy. Such attacks need to be amplified in some way to be successful; that is, the adversary's use of data for the intended purpose must be considerably smaller than the individual's data.

b) Depletion of bandwidth: Typically, adversary-controlled zombies overwhelm their victim's networks with IP traffic in a coordinated dispersed attack. Generally speaking, the intention is to prevent the victims from being reached by others and/or to generally hinder their capacity for communication.

Typically, these types of attacks use TCP, UDP, or ICMP and rely on flooding the victim with packets at the fastest data rate possible[16].

c) Prefix hijacking and black-holing: Prefix hijacking occurs when an unfriendly, confused, or corrupted autonomous system (AS) advertises invalid routers in an attempt to persuade other ASs to forward their traffic to it. [16]. This may lead to "black-holing," a situation in which all traffic directed toward the malicious AS is just rejected. This attack works well in IP networks because it is hard for routers to identify and fix a compromised routing configuration.

H. Countermeasures Techniques for DOS and DDOS Attack

a) Attack by Reflection

An NDN network records the information and clears the PIT value each time it "overhears" a data transmission on an outgoing interface IFx for which it has a current PIT (Pending Interest Table) value on the receiving port IFx. Keep in mind that the associated PIT entry will have flushed by the time another copy of the same information is given via the outgoing interface (IFy) for that PIT entry. In such a case, the copy will be discarded. This feature makes sure that, even in cases where the original interest was broadcast, different NDN routers on the same broadcast domain do not deliver the same content more than once.

b) Depletion of bandwidth

This attack would have extremely little effect. After the content is first downloaded from the source, it is cached at on-the-way routers, from which it is later retrieved by interested parties. As a result, the network would restrict how many interests could reach the victim.

c) Prefix hijacking and black-holing

NDN is resistant to prefix hijacking-based black-holing. Compared to their IP counterparts, NDN routers have access to a limited amount of information, which they can utilize to identify irregularities in the content distribution process. You may tell whether a prefix has been hijacked by looking at the number of unsatisfied (expired) interests, as each content takes the same path as the interest that requested it. Furthermore, NDN routers monitor data on each link's and interface's performance for a particular prefix, and they modify their transmitting plan in response to these statistics.. Routers can investigate topological redundancy through multipath forwarding by detecting and eliminating loops. Because multipath routing enables routers to attempt alternate paths in response to prefix hijacking, it further lessens its impact. This raises the likelihood that interests will be forwarded via a path unaffected by the assault. Advertising fictitious routes in NDN, as opposed to IP, prevents the adversary from launching a loophole attack. In summary, routers can identify and respond to network problems fast (i.e., at the RTT scale), detect and thwart hijacking attacks, and include congestion into forwarding decisions thanks to the NDN forwarding layer [16].via a path unaffected by the assault. Advertising fictitious routes in NDN, as opposed to IP, prevents the adversary from launching a loophole attack. In summary, routers can identify and respond to network problems fast (i.e., at the RTT scale), detect and thwart hijacking attacks, and include congestion into forwarding decisions thanks to the NDN forwarding layer [16].

I. Interesting Flooding Attack:

A flooding attack's primary objective is to seize control of network resources and prohibit authorized users from accessing them. A great deal of interesting messages are transmitted to do this. Such interest messages generate PIT entries in every NDN network from origin to target. Because such entries remain in PIT for longer lengths of time, real consumers are unable to access PIT. Gasti et al. [16] hypothesized three forms of interest flooding attacks: kind 1 (the current or fixed), kind 2 (continuously produced), and kind 3 (inactive). Such assaults depend upon interest messages, which are used in interest flooding attacks. An intruder repeatedly sends interest packets for a collection of kind 1 prior contents. Because of in-network caching, the surrounding NDN routers cache these items.

A kind 2 interest overflow assault involves sending demands on the randomly generated product. Because the contents are created constantly, the CS of NDN routers is not met. Requests for these contents produce entries in the PIT of NDN routers from origin to target. The newly created entries are retained in PIT till the routers receive the data packet corresponding to the mentioned PIT values. The producer creates dynamic material for these interest packages. To meet these requirements, the producer's resources are spent in an attack scenario. This attack has a significant impact on customers, routers, and producers.

The kind-3 interest overflow assault makes requests for content that does not exist. The interest bits about inactive content do not satisfy PIT parameters. Such entries stay in PIT till they expire, preventing the legitimate consumer from using it. This attack is more damaging than the second kind since the PIT information it generates remains in PIT until the timeout, which is often long. [23].

J. Countermeasure Techniques for Interest Flooding Attacks Three algorithms are proposed:

a) token bucket with interface-specific parity; b) Rewards depend on satisfaction; and c) satisfaction-based opposition algorithm. The basis of all three techniques is limiting the total quantity of interest bits that can be transmitted via every port. With one exception—signals designated to every output port are equally dispersed to every receive port—the first approach is comparable to the conventional signal pooling scheme. The second way, each interface acquires information from previously unfilled interest packets. The router's network gateway monitors the satisfaction ratio of every interface and permits interest packets according to this percentage. A random number generator is used to determine the likelihood of deleting an interest signal. The likelihood of an interest packet being discarded is governed by an unpredictable factor determined by the contentment percentage. In the third technique, all receiving port has a limit to meet the desired message. The neighbor's downstream set their restrictions based on the announcements made by routers about these constraints. This method aids in improving the statistics of valid interfaces. Push-back based on satisfaction works better at reducing interest flooding attacks than the other two methods combined. These methods employ a probabilistic filter on the malicious interface, potentially causing legitimate packets to be negatively impacted.

The PIT size was employed as a parameter to identify interest flooding attacks. Every interface's satisfaction ratio is kept track of by the router, which then permits interest packets according to this percentage. Therefore, a brief spike in traffic from a genuine user may also set off a detection method, leading to a negative result. The method of Naveen et al. [23] is therefore superior in terms of detection accuracy.

V. CONCLUSION

This survey research examined the many kinds of storage attacks in the ICN and NDN architectures. This survey looks at several kinds of assaults that have happened recently and discusses the security steps that can be taken to prevent them. Thus, the survey report offers a variety of strategies to efficiently manage attacks without interfering with ICN nodes, including the goal of this paper, which is to provide researchers with domain expertise on the particular problems related to NDN security. The researchers are motivated to work in this field by the open research issues that are offered.

REFERENCES

[1] Jie Zhou, Jiangtao Luo, Junxia Wang, Liang lang Deng, N, "Cache Pollution Prevention Mechanism Based on Deep Reinforcement Learning in NDN", Journal of Communications and Information Networks, Vol.6, No.1, Mar. 2021.

[2] Naveen Kumar, Shashank Srivastava," IBPC: An Approach for Mitigation of Cache Pollution Attack in NDN using Interface-Based Popularity", Research article, July 12th, 2021

[3] Abdelhak Hidouri, Mohamed Hadded, Nasreddine Hajlaoui, Haifa Touati, Paul Mühlethaler," Cache Pollution Attacks in the NDN Architecture: Impact and Analysis," - 29th International Conference on Software, Telecommunications and Computer Networks, Sep 2021

[4] Muhammad Umar Satta, Rana Asif Rehman " Interest Flooding Attack Mitigation in Named Data Networking based VANETs," 2019 International Conference on Frontiers of Information Technology (FIT)

[5] Muhammad Ali Naeem, Rehmat Ullah, Yahui Meng, Rashid Ali and Bilal Ahmed Lodhi, " Caching Content on the Network Layer: A Performance Analysis of Caching Schemes in ICN-based Internet of Things", IEEE Internet of Things Journal · September 2021

[6] Mohammad Shahrul Mohd Shah1 , Yu-Beng Leau 1 ,Mohammed Anbar , And Ali Abdulqader Bin, " Security and Integrity Attacks in Named Data Networking: A Survey," 23 January 2023, date of current version 26 January 2023.

[7] Arif Hussain Magsi, Leanna Vidya Yovita, Ali Ghulam, Ghulam Muhammad, and Zulfiqar Ali, " A Content Poisoning Attack Detection and Prevention System in Vehicular Named Data Networking," IEEE Sustainability 2023, 15, 10931. https://doi.org/10.3390/ su151410931

[8] Guanglin Xing, Jing Chen, Rui Hou, Lingyun Zhou, Mianxiong Dong, Deze Zeng, Jiangtao Luo, and Maode Ma, " Isolation Forest- Based Mechanism to Defend against Interest Flooding Attacks in Named Data Networking", IEEE Communications Magazine • March 2021

[9] Ren-Ting Lee, Yu-Beng Leau, Yong Jin Park & Mohammed Anbar,"A Survey of Interest Flooding Attack in Named Data Networking: Taxonomy, Performance and Future Research Challenges," Taxonomy, Performance and Future Research Challenges, IETE Technical Review,01 Aug 2021

[10] Amin Karami, Manel Guerrero-Zapat," An ANFIS-based cache replacement method for mitigating cache pollution attacks in Named Data Networking", Journal of Computer Networks January 28, 2015

[11] Reza Tourani, Satyajayant Misra, Travis Mick, Gaurav Panwar," Security, Privacy, and Access Control in Information-Centric Networking: A Survey", Cisco Visual Networking Index:Forecast and Methodology

[12] Mauro Conti , Paolo Gasti , Marco Teoli, " A lightweight mechanism for detection of cache pollution 4 attacks in named data networking,"Computer Network, Sep 2013

[13] Alex Afanasyev, Jeff Burke, Tamer Refaei, Lan Wang, Beichuan Zhang, Lixia Zhang " A Brief Introduction to Named Data Networking ", d by US National Science Foundation under award CNS-1719403, CNS-1629769, CNS-1629009 and CNS-1629922.

[14] Zhiwei Xu, Bo Chen , Ninghan Wang,, Yujun Zhang, Zhongcheng L," ELDA: Towards Efficient and Lightweight Detection of Cache Pollution Attacks in NDN", 10 Nov 2015.

[15] Lin Yao , Zhenzhen Fan , Jing Deng , Fellow, IEEE, Xin Fan , Senior Member, IEEE, and Guowei Wu," Detection and Defense of Cache Pollution Attacks Using Clustering in Named Data Networks" Ieee Transactions On Dependable And Secure Computing, Vol. 17, No. 6,November/December 2020

[16] Paolo Gasti Gene Tsudik Ersin Uzun Lixia Zhang," DoS & DDoS in Named-Data Networking", 7 Aug 2012

[17] Kaiping Xue ,Jiayu Yang, Qiudong Xia, David S. L. Wei Jian Li, Qibin Sun," CSEVP: A Collaborative, Secure, and Efficient Content Validation Protection Framework for Information-Centric Networking," IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 19, NO. 2, JUNE 2022

[18] Lin Yao, Yujie Zeng, Xin Wang, Ailun Chen, and Guowei Wu," Detection And Defense Of Cache Pollution Based On Popularity Prediction In Named Data Networking," IEEE Transactions On Dependable And Secure Computing,2019

[19] Alberto Compagno, Mauro Conti Et Al," A Proactive Cache Privacy Attack On NDN," NOMS 2020 - 2020 IEEE/IFIP Network Operations And Management Symposium

[20] Gergely Acs , Mauro Conti, Paolo Gasti, Cesar Ghali, Gene Tsudik, And Christopher A. Wood , " Privacy-Aware Caching In Information- Centric Networking" Ieee Transactions On Dependable And Secure Computing, Vol. 16, No. 2, March/April 2019

[21] Qichao Xu , Zhou Su , Kuan Zhang, and Peng Li," Intelligent Cache Pollution Attacks Detection for Edge Computing Enabled Mobile Social Networks", Ieee Transactions On Emerging Topics In Computational Intelligence, Vol. 4, No. 3, June 2020

[22] Hani Salah,Mohammed Alfatafta, Saed SayedAhmed, Thorsten Strufe," CoMon++: Preventing Cache Pollution in NDN Efficiently and Effectively", IEEE 42nd Conference on Local Computer Networks 2017

[23] Naveen Kumar, Ashutosh Kumar Singh, Abdul Aleem and Shashank Srivastava," Security Attacks in Named Data Networking: A Review and Research Directions", Security attacks in named data networking: A review and research directions. Journal Of Computer Science And Technology 34(6): 1319–1350 Nov. 2019. Doi 10.1007/S11390-019- 1978-9.

[24] Vanitha.k.s, Dr.s.v.Uma , Mahidhar.s.k, "Distributed Denial of Service: Attack techniques and mitigation", 978-1-5386-0615-5/17/$31.00 ©2017 IEEE.