

A Secure and Optimal Content Validation and Protection Scheme for Information Centric Networks

Prof. Aravinda Thejas Chandra¹, Bommineni Lakshmi Ramya², Dhanunjaya Reddy Sai Lavanya³
Bhoomika R⁴, Chethana S⁵

Professor, Department of Information Science and Engineering¹
Students, Department of Information Science and Engineering^{2,3,4,5}
SJC Institute of Technology, Chickballapur, India

Abstract: *Information-Centric Networking (ICN) is a new Internet infrastructure architecture that is primarily created to accommodate the user demand for content delivery using in-network caching. ICN is vulnerable in that attackers can introduce poisoned content into the network and isolate users from reliable content sources, even if it helps users access content and makes better use of network resources. This attack can be effectively stopped by implementing signature verification in each router, however doing so comes at a significant computational cost. From a single route standpoint, existing ICN techniques reduce verification overhead, but they do not take into account integrating resources for cooperative content authentication and cyber self-defense. From a single route standpoint, existing ICN techniques reduce verification overhead, but they do not take into account integrating resources for cooperative content authentication and cyber self-defense. In this paper, we propose the implementation of a multi-router collaborative security mechanism for ICN using a collaborative, safe, and effective content validation protection architecture called CSEVP. On the one hand, we perform content verification by probabilistically selecting a router that is a part of the transmission path in order to offload the computing burden of content verification from a single router to numerous ones.*

Keywords: Information-centric networking, content poisoning attacks, validity verification, and authentication are the terms used in the index

I. INTRODUCTION

In order to address the conflicts between the current constrained bandwidth of IP networks and the increasing user demand for content delivery, INFORMATION-CENTRIC Networking (ICN) has been proposed as a next-generation network design. Instead of using network addresses to discover and receive content, ICN uses content names, which refocuses the network's attention from where content is to what user desire. All intermediate routers can also cache contents and instantly respond to user requests. The aforementioned benefits of ICN, meanwhile, also present new security issues. The Content Poisoning Attack (CPA) is a common problem. Unverified and tainted contents have the potential to be cached by routers and remain in the network throughout transmission, which impacts the legitimacy of contents in the ICN network since intermediate routers can independently pick and cache materials as they transmit. By impersonating a content provider and introducing contaminated content into the routers' cache, attackers can use this vulnerability to perform CPA attacks. The ICN itself may unintentionally disseminate these poisonous substances throughout the network. The proliferation of harmful content could potentially deplete several network cache resources and cut off consumers from legitimate contents. By impersonating a content provider and introducing contaminated content into the routers' cache, attackers can use this vulnerability to perform CPA attacks. The ICN itself may unintentionally disseminate these poisonous substances throughout the network. The proliferation of harmful content could potentially deplete several network cache resources and cut off consumers from legitimate contents. The standard ICN uses digital signature techniques to safeguard content validity in order to address this security issue

When an intermediate router encounters content that has not been verified, it performs signature verification to confirm the content's legitimacy. However, asymmetric cryptography has an excessively high computational overhead. A router cannot support such high overhead for signature verification if it rapidly receives large amounts of unconfirmed content. Gasti et al. proposed to use solely the HMAC values of the content for content validity verification, which can drastically minimize the verification overhead, in order to improve the existing signature-based authentication technique. However, the new authentication method also introduces fresh security holes. All routers in Gasti et al.'s approach calculate HMAC values using the same key, making it so that an attacker only has to learn one key in order to launch a successful attack.

According to authentication feedback from users, some different non-signature-based authentication techniques handle polluted content in the cache. To reduce content poisoning, Ghali et al. using a lightweight ranking system. The ICN network's routers working together to validate contents is a workable solution to this issue [8]. It is clear that exchanging authentication results for material can efficiently cut down on needless repetition of verifications. The router can divulge the authentication results to others after having authenticated the content. Other routers that receive the same material can rapidly determine if it is genuine based on the shared verification findings without the need for repeated cryptographic operations.

II. RELATED WORK

In-Network The main component of ICN, caching, excels at accelerating content transmission. However, the ability to cache also raises security concerns that must be resolved. One of these, access control, can be resolved using broadcast encryption, public-key facilities, certificateless group signatures, or emerging technologies like blockchain. When caching data at intermediate routers, the issues related to data privacy must also be taken into consideration. To stop customer privacy leakage, Li et al. and Wang et al. suggested flow-based and session-based control techniques, respectively. Cache Pollution Attack attempts to lower the network's cache using rate by filling caches with a large number of unpopular contents. Cache shield was developed by Xie et al. to evaluate this attack by examining the popularity of the data in the network cache. Yao et al. successfully used grey forecast to anticipate the future popularity of each cached piece of material by taking advantage of the regularity of past Interests and popularity. It efficiently prevents non-popular items from encroaching into the cache by detecting content pollution. Statistical and machine learning techniques are effective security against this attack. Clustering and Bayesian analysis modes were used by Nguyen et al. to accept CFA attacks that are taking place in the network using learning techniques.

We concentrate on Content Poisoning Attack (CPA) in this study. In a CPA, the attacker transfers the contaminated contents to the ICN network and stores them in the routers' content store (CS). These tainted materials, which are dispersed throughout the ICN network, have accurate content names that can correspond to the user's interest requests. The tainted material can be matched, given to users, and some intermediate routers may store them in their CS when interest requests submitted by users with the relevant content name reach these routers. Due to the contaminated items taking up a lot of cache resources, this attack may block users from accessing valid source content and may also harm users indirectly.

III. SYSTEM MODEL

3.1 System Model

We take into account an ICN network made up of three components in our scheme: routers under the supervision of an ISP

A. Routers Managed by an ISP

This type of router offers users and CPs access to the ICN network. It provides effective content delivery with the aid of an in-network cache. Additionally, it is in charge of examining the information delivered over the network and removing any poisonous information quickly enough to stop it from being transmitted. Edge routers and cache-enabled routers are the two main categories of routers in the ICN network. If the requested data are cached, cache-enabled routers will forward interesting packets and reply to requests. All contents from CPs will transit through the edge router before being sent to the network in order to identify the source of the poisoned contents. In order to prevent retroactive punishment, edge routers identify them to show from which edge router the content enters the network.

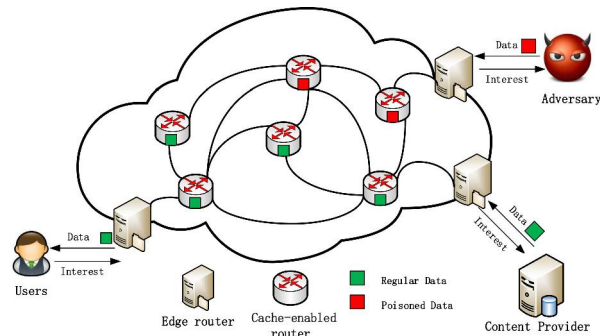


Fig. 1. System Model

B. Content Servers Maintained by Content Providers

These companies develop content and distribute it via the ICN network, similar to Netflix and YouTube. Before publishing, CPs will combine signature and other verification information with contents to make it easier for intermediate routers to verify the validity of the content. However, it is assumed that some adversaries in the ICN network carry out content pollution attacks, in which they pose as phone content providers, reply to interest packets sent by the edge routers, and then send back tainted content to carry out the attack.

C. Users

These people consume content and get it from CPs or ICN networks as desired.

3.2 Assurances of Security

According to our plan, ISP-owned routers are in charge of distributing content, spotting and removing contaminated materials from the network. We assume that all routers are trustworthy of one another and primarily concentrate on tackling the content poisoning attack used by end-hosts. This presumption is plausible because

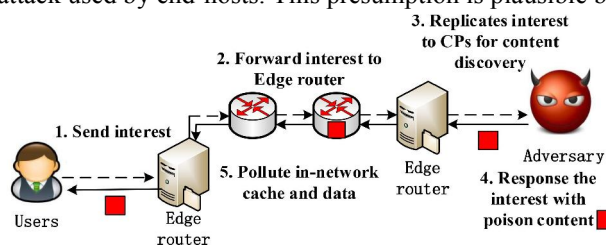


Fig. 2. Replication of Interest-Based Content Poisoning.

In actual network circumstances, it is difficult for adversaries to attack intermediate routers, and it is exceedingly difficult to carry out a content contaminant assault directly on the router. In various other relevant literatures, such as Kim et al.'s scheme (often known as the "Kim Scheme" for short), ABE, and LASA, this security assumption is also stated. At the conclusion of Section V, we provide a trust mechanism as an addition to the suggested scheme to address the scenario in which routers do not trust one another. This scenario is also taken into consideration.

Owners of contents, known as CPs, are thought to be dishonest. Genuine CPs reply to the ICN network's request and transfer material via edge routers. When given the chance to reply to requests, some adversaries who pose as content providers introduce poisonous data into the network. A CP's

normalcy or danger cannot be determined until all of its contents have been thoroughly examined. As a result, ISPs cannot trust CPs, and routers must check material from all sources.

3.3 Design Goals

Our system is built to quickly identify Content Poison Attacks and safely thwart attacks on the ICN.

As was already explained, the in-network cache in CPA contains the poison contents. When users' queries have the same name as the poisoned contents, they will receive infected contents. When ICN cache contains poisoned contents as a result of content poison attacks, users experience is poor.

The attacker injects poisoned contents into the ICN network, as shown in Fig. 2. The edge router forwards the interest packet to the CPs that control the requested content when a user requests nonexistent content from the ICN network. In certain situations, an enemy disguising itself as a content provider will intercept the interest packet and respond to the user's request with poisoned content as soon as possible. Infected content travels into the ICN network and contaminates the in-network caches if it first reaches the edge router without performing any validity checks. When constructing a pending interest table, the edge router will drop the appropriate contents from standard content providers.

- Security: All poisoned items must be identified and removed from the network cache before they reach the sides of users in order to safeguard the ICN network from the damage caused by CPA. Additionally, the plan must the attacker who starts the CPA and stop the attackers from re-entering the network with their contaminated content.
- Efficiency: The method must make the best use of network resources for content verification computations in order to ensure efficient content validation. This requires it to make the most of each router's computational capabilities while minimize the use of redundant verification calculations.

IV. PROPOSED SCHEME

4.1 Overview

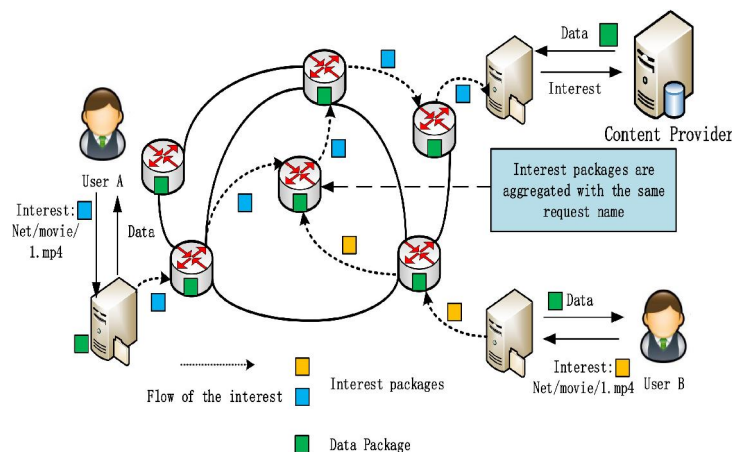
In our system, content packet signatures are used by intermediate routers to validate the contents. We have taken two key strategies to reduce signature verification overhead in order to avoid the significant overhead brought on by asymmetric signature authentication.

In order to capture and share verification results, our scheme first introduces the bloom filter. In instance, by querying the bloom filter with the signature of valid contents, routers may quickly assess the legitimacy of material. Every router can share its bloom filters with its nearby routers from time to time in the meantime. Routers can spread verification information among themselves with less communication overhead by broadcasting and merging bloom filters.

On the other side, the approach provides a fair distribution of authentication jobs by using a probabilistic disjoint verification mechanism. In order to guarantee that every piece of content is genuine and has been validated once before reaching users, each router on the path back to the user has the same probability. Following an intermediate router's verification of the content's validity, subsequent routers can transmit content directly and without further processing once they have confidence in the verification results.

We also provide methods for locating and punishing enemies. The edge router from which each piece of material enters the network is identified by a marker. In order to locate content access records at the edge router, an intermediate router follows the label marked when it discovers incorrect material.

4.2 Content Punishment



- CP Registration: A reliable CP must register with a reputable third-party central authority (CA) for his or her identification and certificate prior to posting contents into the ICN network.

- Publishing Contents: In response to requests from the ICN network, the CPs publish content to the edge router with its certificate. This content consists of a series of chunks. The edge router checks the authenticity of the certificate and the validity of the content packet's signature when it gets these content chunks. If so, the edge router forwards chunks into the ICN network and places the information it needs for content tracing in the reserved fields of the packet. If not, it throws them away.

4.3 Contents Authentication Process

The ICN network first selects an intermediate router to authenticate the content using a probabilistic verification protocol when CPs publish unverified material and the content enters the ICN network through an edge router. For quick verification, the chosen intermediate router searches the cached bloom filter including the results of the verifications performed by it and other routers. If not, it checks the information and saves the findings in a bloom filter for reuse and sharing.

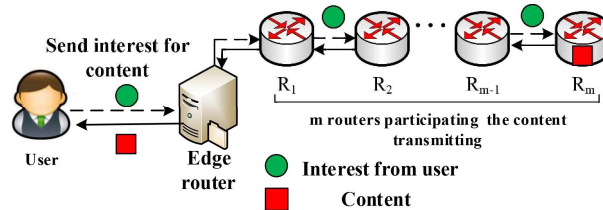


Fig.3. Protocol for Probabilistic Verification

- Probabilistic Verification Protocol: The Probabilistic Verification Protocol ensures that before content reaches the user, it must be checked once with the same probability for each router by cooperating with intermediate routers on the reply content path to carry out a probabilistic disjoint verification. We use interest packets to record the number of hops routed to the hit router or CP in the ICN and compute the probability of each router in order to obtain an adequate probabilistic verification. The number n , which we define as the number of hops in the interest packet, also denotes the number of intermediary routers taking part in the probabilistic verification. As seen in Fig. 4, n is numbered from the first intermediate router transmitting the interest packet for the reply content from a CP through the edge router. Due to the fact that all items cached by routers are designated as verified, we do not analyze a scenario in which the interest is met at the intermediate router.

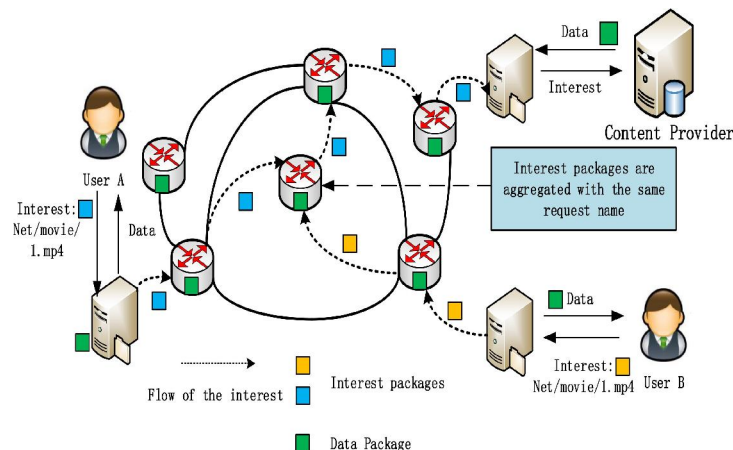


Fig.4. The problem with aggregating interests.

- Verification and Sharing Results Based on Bloom Filter: An intermediate node uses a bloom filter to quickly verify transmitted material when authenticating it. The initialization of the bloom filter, its application, and the sharing of authentication data based on the bloom filter are all covered in the following sections. The steps of the procedure are as follows:
- Initialization of the bloom filter: Before verifying any material, each intermediate router must construct a bloom filter. A bloom filter with the size m and hash function is initiated by a router using the operator $bf \text{ BF}$.

Set up (m.). To ensure significant effectiveness, the ISP must establish a maximum false positive rate for the router's bloom filter, taking into account the bloom filter's inherent tendency to produce false positive results.

- Verification based on the bloom filter: If a piece of material has been verified as legal, it will be marked with the corresponding tag to show that it has been, and the content name and associated hash value will be saved in the bloom filter. It will initially check to see if the content is in its bloom filters before selecting an intermediate router to verify the content. We outline how to use the bloom filter in Algorithm to verify content. If there is no appropriate signature saved in the bloom filter, the content must be confirmed using signature and hash verification. The intermediate router will specifically check the content's signature. Verification of an Algorithm Using a Bloom Filter

V. PERFORMANCE ANALYSIS

We examine the effectiveness of the suggested plan in this section. We first evaluate the probabilistic disjoint verification protocol's computation resource overhead and simulate the results of allocating computation resources in a virtual network. Then, we compare our scheme to the standard ICN scheme and the scheme in and analyze the overheads of the bloom filter-based content verification in our scheme.

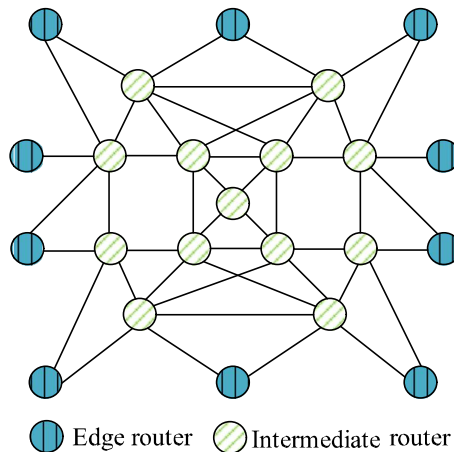


Fig. 5. Topology in the simulation.

the intermediary router's overhead.

The next step is to confirm that the probabilistic verification protocol can spread the network's local verification pressure evenly over the entire network and reach a specific level of integration of computer resources. We run a stress test on the accuracy of the content in a simulated network environment to evaluate our protocol. It has 23 routers, with 10 edge routers and 13 middle routers, as indicated in. We abstract the topology into a grid one to ease the verification pressure of the network in the following. The number of verification calculations performed on each node is recorded by the grid topology. The number of times this router has been verified is shown by the grid's darker color.

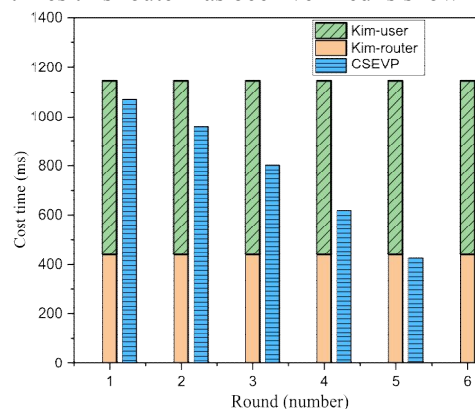


Fig. 6. Verification cost of multi-router collaboration.

In this part, we assess how our collaborative authentication approach has improved verification efficiency. We examine our scheme's verification delay and storage cost. At the same time, we examine the additional communication overhead brought on by information interaction during collaboration using network simulations. Evaluation of storage Bloom filter will speed up verification while adding more storage overhead. We tested the reasonableness of the bloom filter's space occupation by simulating our plan in the ICN network environment.

VI. RESULTS

Information-centric networking (ICN) is a network architecture that is designed to distribute and retrieve content based on its name or identifier, rather than its location. This approach is different from traditional networking, which relies on IP addresses and hosts. In ICN, content is broken down into chunks, and each chunk is assigned a unique identifier. These identifiers can be used to retrieve the content from any location where it is available. To ensure the security and integrity of content in ICN, it is important to have a framework for collaborative content validation and protection. Such a framework would involve multiple entities in the network, including content producers, content consumers, and intermediaries. These entities would work together to verify the authenticity and integrity of the content, and to protect it from unauthorized access and modification.

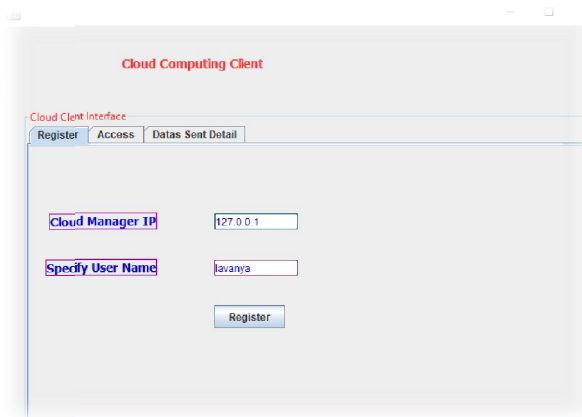


Fig.7. Registration details of user

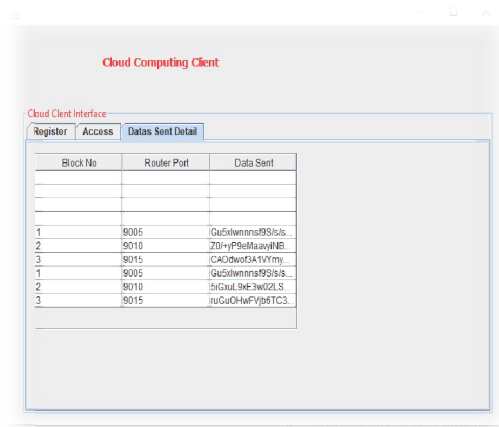
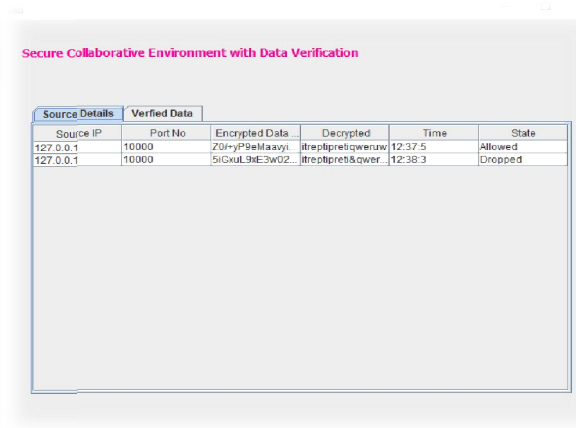


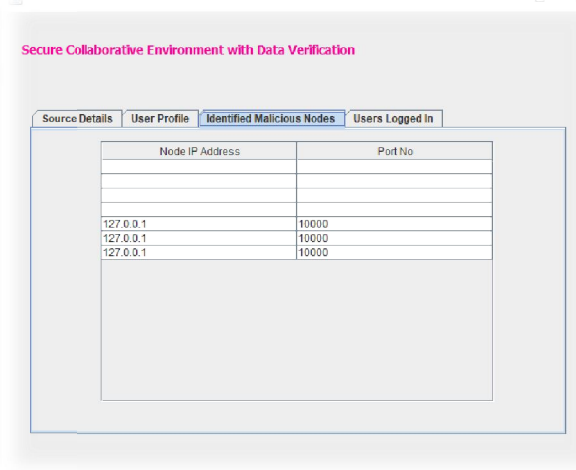
Fig.8. Details of data sent by user to router



Secure Collaborative Environment with Data Verification

Source Details		Verified Data			
Source IP	Port No	Encrypted Data	Decrypted	Time	State
127.0.0.1	10000	Z0r-yP8eItaaxv	ltretpretiqwarw	12:37:5	Allowed
127.0.0.1	10000	5iGwUL3hE3wO2	ltretpret&zwef	12:38:3	Dropped

Fig.9. Source details in Router portal



Secure Collaborative Environment with Data Verification

Identified Malicious Nodes	
Node IP Address	Port No
127.0.0.1	10000
127.0.0.1	10000
127.0.0.1	10000

Fig.10. Router identified the malicious nodes

VII. CONCLUSION

In this paper, we presented a collaborative, secure, and efficient content validation protection scheme, called CSEVP, for ICN. In CSEVP, we implement collaborative authentication for content validity among multiple routers in the ICN network. Furthermore, By leveraging a probabilistic verification protocol, routers participating in transmission can share the pressure of validity verification. Also, the introduction of bloom filter helps routers share verification results and increases the efficiency of validity verification. Via experimental analysis, the results demonstrate that CSEVP is a promising solution for content validation protection in ICN, which meets the security requirements and also guarantees good enough efficiency

REFERENCES

- [1]. K. Xue et al., "A secure, efficient, and accountable edge-based access control framework for information centric networks," IEEE/ACM Trans. Netw., vol. 27, no. 3, pp. 1220–1233, Jun. 2019.
- [2]. B. Nour, H. Khelifi, R. Hussain, S. Mastorakis, and H. Moun gla, "Access control mechanisms in named data net-works: A comprehensive survey," ACM Comput. Surveys, vol. 54, no. 3, pp. 1–35, 2021.
- [3]. H. Huang, Y. Wu, F. Xiao, and R. Malekian, "An efficient signature scheme based on mobile edge computing in the NDN-IoT environment," IEEE Trans. Comput. Social Syst., vol. 8, no. 5, pp. 1108–1120, Oct. 2021.

- [4]. S. Misra, R. Tourani, F. Natividad, T. Mick, N. E. Majd, and H. Huang, "AccConF: An access control framework for leveraging in-network cached data in the ICN-enabled wire-less edge," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 1, pp. 5–17, Jan./Feb. 2019.
- [5]. B. Bera, S. Saha, A. K. Das, and A. V. Vasilakos, "Designing block chainbased access control protocol in IoT-enabled smart-grid system," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5744–5761, Apr. 2021.
- [6]. J. Ni, K. Zhang, and A. V. Vasilakos, "Security and privacy for mobile edge caching: Challenges and solutions," *IEEE Wireless Commun.*, vol. 28, no. 3, pp. 77–83, Jun. 2021.
- [7]. L. Yao, Y. Zeng, X. Wang, A. Chen, and G. Wu, "Detection and defense of cache pollution based on popularity prediction in named data networking," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 6, pp. 2848–2860, Nov./Dec. 2021.
- [8]. N. Yang, K. Chen, and M. Wang, "SmartDetour: Defending blackhole and content poisoning attacks in IoT NDN networks," *IEEE Internet Things J.*, vol. 8, no. 15, pp. 12119–12136, Aug. 2021.
- [9]. Elgabli, A., Fekih, A., & Khemakhem, M. (2021). Collaborative security framework for information-centric networking. *Journal of Network and Computer Applications*, 171, 102912.
- [10]. Zrelli, R., & Koufi, N. (2021). A collaborative approach for securing content distribution in information-centric networks. *Wireless Personal Communications*, 120(1), 115-129.
- [11]. Peng, Y., & Chen, H. (2022). A Collaborative and Secure Content Delivery Scheme Based on Blockchain in ICN. In *Proceedings of the 6th International Conference on Communication and Information Processing (ICCIP 2022)* (pp. 62-68). ACM.
- [12]. Wang, X., Li, X., Li, Z., Li, T., & Li, Y. (2021). A Collaborative and Secure Content Distribution Framework for Information-Centric Networks. *IEEE Transactions on Network and Service Management*, 18(2), 1435-1449.
- [13]. Li, T., Li, Z., Li, X., Li, Y., & Li, J. (2023). A Secure and Efficient Collaborative Content Validation Framework for Information-Centric Networks. *IEEE Transactions on Dependable and Secure Comput* 20(1), 70-85.