IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

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

Prof. Aravinda Thejas Chandra[1], Bommineni Lakshmi Ramya[2], Dhanunjaya Reddy Sai Lavanya[3]
Bhoomika R[4], Chethana S[5]
Professor, Department of Information Science and Engineering[1]
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

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. Moungla, "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 predic-tion in named data networking," IEEE Trans. Dependable Secure Comput., vol. 18, no. 6, pp. 2848–2860, Nov./Dec. 2021.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, May 2023

[8]. N. Yang, K. Chen, and M. Wang, "SmartDetour: Defending blackhole and content poisoning attacks in IoT NDN net-works," 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., & Khoufi, 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 Computi 20(1), 70-85.