

User Data-Centric Authentication for Network Data Retrieval

SK. Pujitha¹, Vemula Vigneshwari², Javaji Vijay Kumar³, Vanga Madhu Krishna⁴

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, India¹

Department of CSE, Guru Nanak Institute of Technology, Hyderabad, India^{2, 3, 4}

ABSTRACT: Big data has created a strong demand for secure and efficient data retrieval in modern network environments. Information-Centric Networking (ICN) enables data to be cached within the network, allowing users to retrieve data from nearby cache locations instead of centralized servers. Although this improves performance and reduces delay, it also introduces security threats such as malicious-request attacks and data-poisoning attacks. Existing systems mainly provide authentication only between users and publishers and suffer from increased authentication delay due to dependency on centralized certificate servers. To overcome these issues, this project proposes a secure Data-Centric Authentication framework called DCAuth using the Suspension-Chain Model (SCM). The proposed system integrates certificate collection with packet forwarding to establish secure authentication among users, routers, publishers, and network entities without relying heavily on centralized servers. The framework reduces authentication delay, prevents fake-data propagation, and improves secure big-data retrieval in ICN environments. Experimental analysis shows that DC Auth enhances network security, reliability, and overall performance compared to existing approaches.

KEYWORDS: Information-Centric Networking (ICN), Data-Centric Authentication, Big Data Retrieval, SuspensionChain Model (SCM), DCAuth, Data Poisoning Attack, Network Security.

I. INTRODUCTION

In the modern digital world, billions of mobile devices, sensors, and smart systems continuously generate large amounts of data. This rapid growth of information has introduced the concept of big data, which is characterized by volume, variety, velocity, value, and complexity. Traditional Internet architecture relies mainly on centralized cloud servers for data retrieval, resulting in network congestion, redundant traffic, and increased latency.

To overcome these limitations, Information-Centric Networking (ICN) and Named Data Networking (NDN) architectures were introduced. In ICN, data is cached within the network at Intermediate Physical Entities (IPEs), enabling users to retrieve information from nearby cache locations instead of distant servers. Although this improves efficiency and reduces delay, it also introduces several security issues.

One of the major concerns in ICN is the occurrence of malicious-request attacks and data-poisoning attacks. Attackers may impersonate legitimate users to flood requests or distribute fake data into network caches. Since cached data spreads quickly across the network, fake data can severely impact system reliability and security.

To address these issues, this project proposes a secure authentication framework called DCAuth (Data-Centric Authentication with Suspension Chain). The framework integrates trust establishment, certificate exchange, and packet forwarding mechanisms to provide secure communication among users, routers, publishers, and network entities.

II. LITERATURE SURVEY

Reeves, A., Shaghghi, A., Krebs, S., & Ashenden, D. (2025) This study explores how digital data becomes a legacy after death and highlights the lack of clear policies for managing posthumous data. It emphasizes the importance of transparent and user-controlled systems for secure preservation and distribution of digital assets after death.

Amadeo, M. (2025) This paper explores the integration of Information-Centric Networking (ICN) with in-network computing to improve data delivery, scalability, and security in modern communication systems. The study discusses challenges such as service naming, compute reuse, and secure content distribution while proposing future research directions for ICN-based architectures.

Atalay, T.O., et al. (2025) This research proposes a systematic security framework for Named Data Networking (NDN) by embedding trust directly into the data rather than relying on external communication channels. The study highlights the importance of data-centric security, fine-grained trust management, and secure communication in future network ecosystems.

Menéndez, R., Munoz-Arcentales, A., Salvachúa, J., Aparicio, C., Plaza, I., & Huecas, G. (2025) This paper introduces a next-generation authentication protocol for secure data spaces using decentralized identity verification and self-sovereign identity principles. The proposed framework improves privacy, scalability, interoperability, and secure interactions between participants in distributed digital environments.

III. METHODOLOGY

The core of the proposed system is a secure Data-Centric Authentication framework called DCAuth, which combines certificate management, packet forwarding, and trust establishment in Information-Centric Networking (ICN). The methodology focuses on providing secure communication, reducing authentication delay, and preventing malicious request and data-poisoning attacks during big-data retrieval.

Existing System Disadvantages

- Increased authentication delay due to centralized certificate access.
- Vulnerability to malicious-request attacks.
- Vulnerability to data-poisoning attacks.
- Lack of secure authentication among unpredictable network entities. High dependency on centralized infrastructure.

Proposed System

The proposed system introduces a secure and efficient Data-Centric Authentication framework called DCAuth using the Suspension-Chain Model (SCM) for secure big-data retrieval in Information-Centric Networking (ICN) environments. The primary objective of the system is to provide secure communication and reliable authentication among users, routers, publishers, and Intermediate Physical Entities (IPEs) during data transmission and retrieval. Unlike traditional systems that rely heavily on centralized certificate servers, the proposed framework integrates certificate collection with packet forwarding to establish trust dynamically and efficiently within the network.

The Suspension-Chain Model (SCM) combines Certificate Authority (CA)-based trust and neighbor-based trust to create a secure authentication mechanism. Using this model, every network entity such as users, routers, and publishers is verified through certificate chains before communication occurs. When a user requests data, the request packet contains authentication certificates that are validated at each intermediate node before forwarding the request. This process ensures that only authenticated users and trusted entities can participate in network communication.

Another important feature of the proposed framework is the reduction of authentication delay. Existing systems depend on centralized servers for certificate verification, which increases latency and network overhead. In contrast, DCAuth performs certificate verification directly within the network using neighboring trust relationships, significantly reducing communication delay and improving overall network performance.

The proposed system also improves scalability and reliability in large-scale ICN environments. Since authentication and trust management are distributed across network entities, the framework can efficiently support a large number

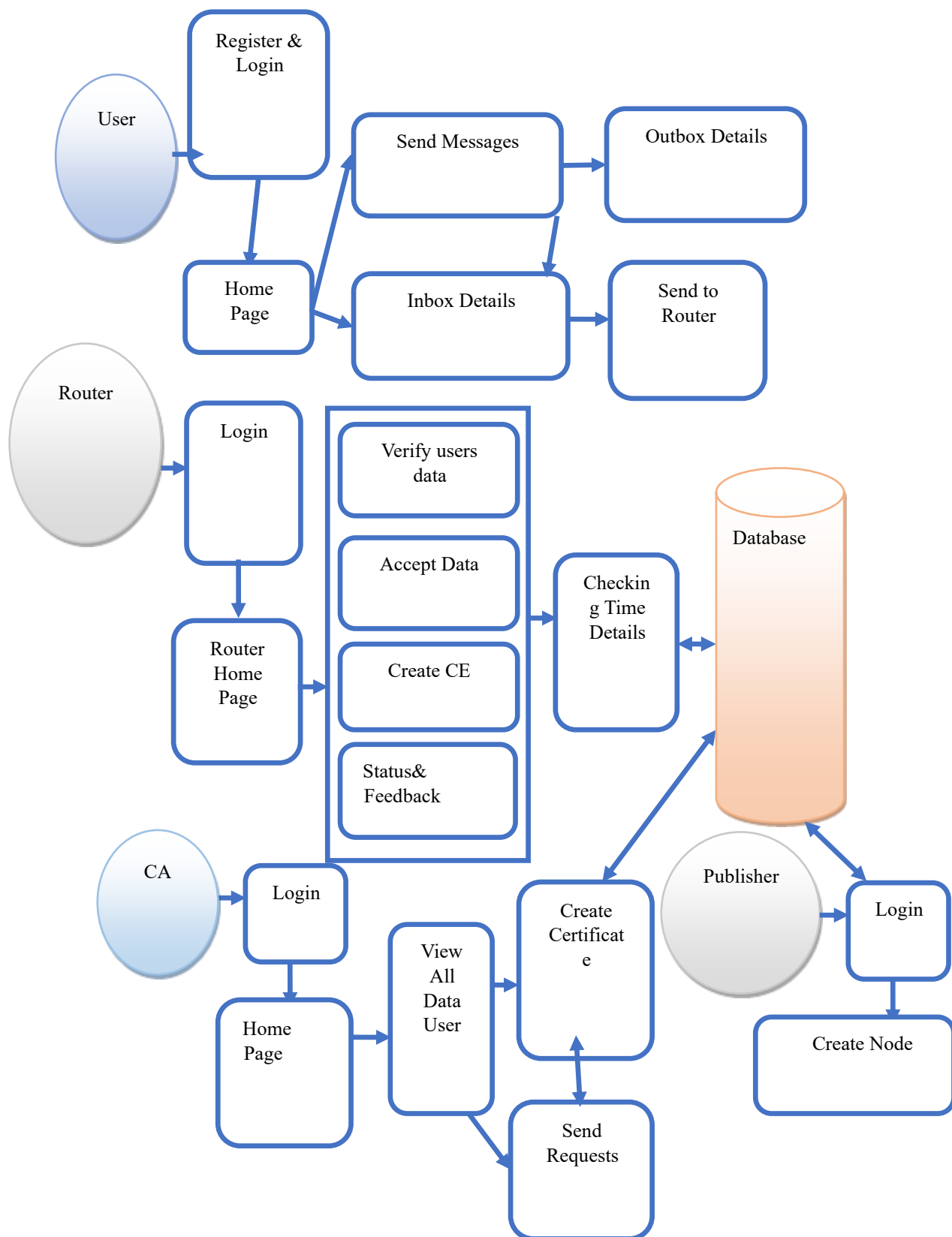
of users and devices without creating excessive load on centralized infrastructure. The integration of secure packet forwarding, certificate management, and trust establishment enhances the overall efficiency of big-data retrieval. Overall, the proposed DCAuth framework provides secure data-centric authentication, efficient certificate verification, reliable packet forwarding, and secure caching mechanisms in Information-Centric Networking environments. The system ensures secure big-data retrieval while improving network security, reducing authentication delay, and preventing unauthorized access and fake-data propagation.

Advantages:

- Secure in-network big-data retrieval.
- Efficient certificate management.
- Reduced latency and improved performance.
- Enhanced trust management in ICN environments.



SYSTEM ARCHITECTURE



The system architecture of the proposed project describes the interaction between users, routers, certificate authorities, publishers, and the database during secure network data retrieval. The architecture is based on the DCAuth mechanism and Suspension-Chain Model (SCM) to provide secure authentication and trusted communication in the network.

Modules Explanation:

1. User Interface:

The user interface provides a simple platform for users, routers, publishers, and administrators to interact with the system.

It includes login pages, dashboards, request forms, and data access controls for secure communication.

2. User Module:

This module allows users to register, login, and request data from the network securely.

Users can send requests and retrieve authenticated data from nearby cache locations.

3. Router Module:

The router module verifies certificates, forwards packets, and caches authenticated data.

It helps reduce network delay and prevents unauthorized packet forwarding.

4. Certificate Authority Module:

This module establishes trust among network entities by generating and validating certificates.

The CA manages authentication between users, routers, and publishers securely.

5. Publisher Module:

The publisher module is responsible for publishing original data into the network.

It responds to authenticated requests and distributes verified data to users.

6. Certificate Management:

This module manages certificate collection, verification, and suspension-chain generation. It ensures secure authentication without depending heavily on centralized servers.

7. Data forwarding and caching:

This module handles secure packet forwarding and in-network caching of verified data.

/Only authenticated data is cached to prevent fake-data propagation.

8. Security & Authentication:

This module implements the DCAuth mechanism using the Suspension-Chain Model (SCM).

It prevents malicious-request attacks and data-poisoning attacks while ensuring secure big-data retrieval.

IV. IMPLEMENTATION

The implementation of “User Data-Centric Authentication for Network Data Retrieval” focuses on developing a secure, reliable, and efficient system for authenticating users and protecting network data in Information-Centric Networking (ICN) environments. The system is designed to ensure secure communication, certificate verification, trusted packet forwarding, and efficient big-data retrieval using the DCAuth framework and Suspension-Chain Model (SCM). The implementation integrates user authentication, certificate management, packet forwarding, secure caching, and trust establishment into a unified and scalable platform.

V. EXPERIMENTAL RESULTS

[Home](#) [Cloud Authority](#) [Router](#) [Publisher](#) [User](#) [Register](#)

USER DATA-CENTRIC AUTHENTICATION FOR NETWORK DATA RETRIEVAL

Fig. Home Page

[Home](#) [Cloud Authority](#) [Router](#) [Publisher](#) [User](#) [Register](#)

USER DATA-CENTRIC AUTHENTICATION FOR NETWORK DATA RETRIEVAL

CLOUD AUTHORITY LOGIN

Email

Password

Fig. Cloud Authority Login Page

[Home](#) [Cloud Authority](#) [Router](#) [Publisher](#) [User](#) [Register](#)

USER DATA-CENTRIC AUTHENTICATION FOR NETWORK DATA RETRIEVAL

ROUTER LOGIN

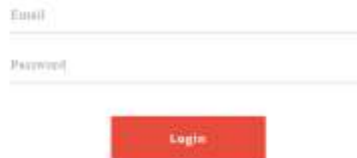
Email

Password

Fig. Router Login Page

USER DATA-CENTRIC AUTHENTICATION FOR NETWORK DATA RETRIEVAL

PUBLISHER LOGIN



Form for Publisher Login with fields for Email and Password, and a Login button.

Fig. Publisher Login Page

USER DATA-CENTRIC AUTHENTICATION FOR NETWORK DATA RETRIEVAL

REGISTER HERE



Form for Registration with fields for Enter Name, Enter Email, Enter Password, dd-mm-yyyy, and Enter Mobile Number, and a REGISTER button.

Fig. Registration Page

USER DATA-CENTRIC AUTHENTICATION FOR NETWORK DATA RETRIEVAL

USER LOGIN



Form for User Login with fields for Email and Password, and a Login button.

Fig. User Login Page

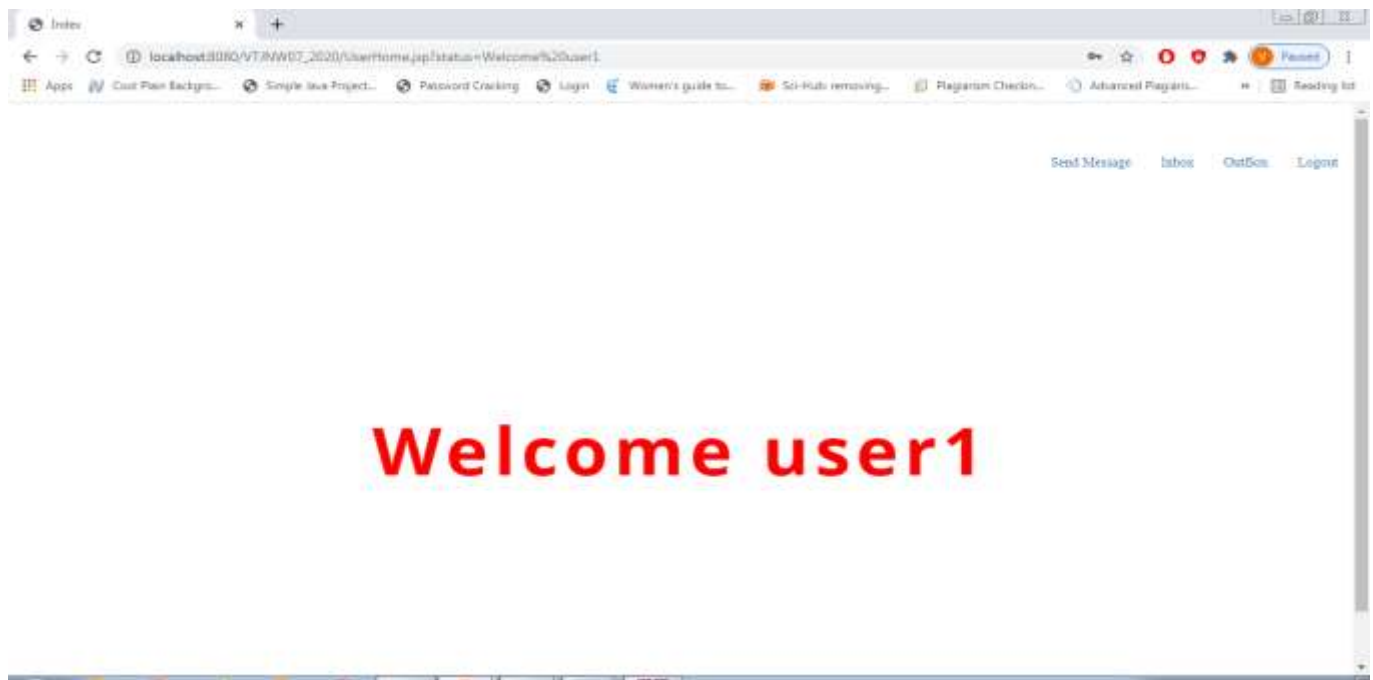


Fig. User Welcome Page

VI. CONCLUSION

Our project “User Data-Centric Authentication for Network Data Retrieval” provides a secure and efficient authentication framework for Information-Centric Networking (ICN) environments. The proposed DC Auth mechanism uses the Suspension Chain Model (SCM) to establish secure communication among users, routers, publishers, and network entities. The system effectively reduces authentication delay and prevents malicious-request and data-poisoning attacks during big-data retrieval. By integrating certificate management, packet forwarding, and secure caching, the framework improves network security, reliability, and scalability. The proposed solution supports efficient in-network data retrieval while minimizing dependency on centralized servers. However, further improvements can be made in areas such as advanced attack detection, large-scale deployment, and performance optimization. Overall, DC Auth provides a strong foundation for future secure and scalable ICN-based communication systems.

VII. FUTURE ENHANCEMENT

In further detail, the insiders cause slightly more bandwidth consumption than the outsiders. It is because around 10 data retrievals are tolerated to discover malicious-request insiders, and users need to retrieve and authenticate the fake data in order to discover data-poisoning insiders. In contrast, the outsiders can be prevented by the first-hop certificate checks from neighbors, as they do not have valid certificates. Therefore, we see that DCAuth achieves a minimal additional delay without incurring additional certificate retrievals and its bandwidth consumption is acceptable for performance while efficiently preventing malicious-request and data-poisoning attacks for in-network big-data retrieval.

REFERENCES

- [1] N. Khan, I. Yaqoob, I. Hashem, Z. Inayat, W. Ali, M. Alam, M. Shiraz, and A. Gani, “Big Data: Survey, Technologies, Opportunities, and Challenges,” *The Scientific World Journal*, Vol. 2014, 2014.
- [2] H. Yin, Y. Jiang, C. Lin, Y. Luo, and Y. Liu, “Big data: Transforming the design philosophy of future Internet,” *IEEE Network*, vol. 28, no. 4, pp. 14-19, July 2014.
- [3] S. Yu, and S. Guo (Eds.), “Big Data Concepts, Theories, and Applications,” Springer 2016, ISBN 978-3-319-27761-5.

- [4] J. Saltzer, D. Reed, and D. Clark, "End-to-end arguments in system design," *ACM Transactions on Computer Systems*, 2 (4), pp. 277-288, 1984.
- [5] S. Yu, M. Liu, W. Dou, X. Liu, and S. Zhou, "Networking for Big Data: A Survey," *IEEE Communications Surveys and Tutorials*, Vol. 19, Issue 1, pp. 531-549, 2017.
- [6] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," *IEEE Communications Magazine*, 50(7), pp. 26-36, 2012.
- [7] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica, "A data-oriented (and beyond) network architecture," *ACM SIGCOMM 2007*, Aug. 2007.
- [8] P. Jokela, A. Zahemszky, C. E. Rothenberg, S. Arianfar, and P. Nikander, "LIPSIN: Line Speed Publish/Subscribe Inter-Networking," *Proceedings of the ACM SIGCOMM 2009*, pp. 195-206, Aug. 2009.
- [9] A. Ghodsi, S. Shenker, T. Koponen, A. Singla, B. Raghavan, and J. Wilcox, "Information-centric networking: seeing the forest for the trees," *Proceedings of the 10th ACM Workshop on Hot Topics in Networks*, 2011.
- [10] S. K. Fayazbakhsh, Y. Lin, A. Tootoonchian, A. Ghodsi, T. Koponen, B. Maggs, K. Ng, V. Sekar, and S. Shenker, "Less pain, most of the gain: incrementally deployable icn," *Proceedings of the ACM SIGCOMM 2013 conference*, pages 147-158, 2013.
- [11] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," *ACM CONEXT'09*, Rome, Italy, Dec. 2009.
- [12] E. AbdAllah, H. Hassanein, and M. Zulkernine, "A survey of security attacks in information-centric networking," *IEEE Communications Surveys & Tutorials*, vol. 17, issue 3, 2015.
- [13] R. Li, and H. Asaeda, "Secure In-Network Big Data Provision with Suspension Chain Model," *IEEE Conference on Computer Communications Workshop on Big Security 2018*, Honolulu, Apr. 2018.
- [14] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest flooding attack and countermeasures in named data networking," *IFIP Networking*, pp. 1-9, 2013.
- [15] A. Compagno, M. Conti, P. Gasti, and G. Tsudik, "Poseidon: mitigating interest flooding ddos attacks in named data networking," *IEEE LCN'13*, pp. 630-638, Oct. 2013.
- [16] T. Nguyen, R. Cogan, and G. Doyen, "An optimal statistical test for robust detection against interest flooding attacks in ccn," *IFIP/IEEE International Symposium on Integrated Network Management (INM)*, pp. 252-260, 2015.
- [17] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "Dos and ddos in named data networking," *In the IEEE ICCCN'13*, pages 1-7, July 30-Aug. 2, 2013.
- [18] C. Ghali, G. Tsudik, and E. Uzun, "Network-layer trust in named-data networking," *ACM SIGCOMM Computer Communication Review*, vol. 44, number 5, Oct. 2014.
- [19] D. Kim, S. Nam, J. Bi, and I. Yeom, "Efficient content verification in named data networking," *ACM Conference on Information-Centric Networking*, pp. 109-116, 2015.
- [20] Z. Su, Y. Hui, Q. Xu, T. Yang, J. Liu, and Y. Jia, "An Edge Caching Scheme to Distribute Content in Vehicular Networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, June 2018.