SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 12 | December 2024 - Peer Reviewed Journal

USER DATA-CENTRIC AUTHENTICATION FOR NETWORK DATA RETRIEVAL

G. Abhishek Reddy[1], G. Kusuma[2], H. Sushumna[3], G. Srujana Bharathi[4]
[1,2,3]UG Scholar, Guru Nanak Institutions Technical Campus, Hyderabad
[4]Assistant Professor, Guru Nanak Institutions Technical Campus, Hyderabad

Article DOI: https://doi.org/10.36713/epra19384
DOI No: 10.36713/epra19384

ABSTRACT

Big data introduces significant demands on network infrastructure, necessitating secure and efficient data retrieval with in-network caching. Information-Centric Networking (ICN) addresses these challenges by caching data across intermediate physical entities (IPEs) and enabling retrieval from nearby sources. However, unpredictable behaviors of users, IPEs, and publishers during data retrieval introduce risks such as malicious data-poisoning and request flooding. Existing systems primarily authenticate between users and publishers, resulting in increased delays and network vulnerabilities. To resolve these issues, we propose DC Auth, a trust model integrating Certificate Authority (CA)-based and neighbor-based trust to achieve efficient and secure data-centric authentication. Simulations confirm that DC Auth significantly reduces delays while enhancing security by mitigating various attacks.

1. INTRODUCTION

The exponential growth in mobile devices and IoT has dramatically increased the demand for big data services. Traditional end-to-end communication models in big data retrieval result in substantial redundancy and latency. ICN provides a transformative solution by caching data closer to users, reducing redundancy and improving latency. However, in-network retrieval introduces new vulnerabilities, such as malicious-request and data-poisoning attacks. Unlike conventional Internet models with predictable trust paths, ICN necessitates a robust authentication framework to mitigate these risks. This research presents DC Auth, a suspension-chain-based trust model designed to secure bigdata retrieval by combining CA-based and neighbor-based trust mechanisms.In today's digital age, the exponential growth in big data and IoT applications has imposed significant demands on network infrastructure. Traditional end-to-end communication models face challenges such as redundancy and latency in data retrieval. Information-Centric Networking (ICN) offers an alternative by caching data across intermediate physical entities (IPEs). However, this architecture introduces vulnerabilities, such as malicious requests and data poisoning attacks, due to unpredictable user and network behaviors.Existing models rely on centralized authentication, leading to higher latency and limited scalability. This paper addresses these challenges by proposing DC Auth, an efficient data-centric authentication system that utilizes a Suspension Chain Model for trust-based in-network authentication.

1.1 OBJECTIVE

The objective of this research is to develop a robust data-centric authentication mechanism for ICN environments. By integrating CA-based trust and neighbor-based trust into a suspension-chain model, DC Auth aims to authenticate unpredictable network entities securely. This system not only ensures data integrity but also minimizes latency and effectively combats malicious attacks in big data networks, providing a practical and scalable solution for modern network infrastructures. The objective of this research is to design a scalable and secure authentication framework for ICN environments. DC Auth integrates CA-based trust with neighbor-based trust mechanisms, enabling dynamic and reliable data retrieval. The system aims to:Minimize authentication delays.Mitigate security threats like request flooding and cache poisoning. Ensure seamless scalability and low-latency communication.

1.2 SCOPE OF THE PROJECT

The scope of this project involves developing a scalable framework using a suspension-chain model to secure in-network big data retrieval. DC Auth integrates seamlessly into network environments by utilizing trust-based certificate chains for authentication. Decentralizing trust mechanisms minimizes dependency on centralized servers, ensuring robust security even in dynamic, large-scale networks with low-latency performance. This solution can be applied to diverse ICN-based applications, ranging from IoT ecosystems to cloud computing environments, enhancing overall network resilience and security.

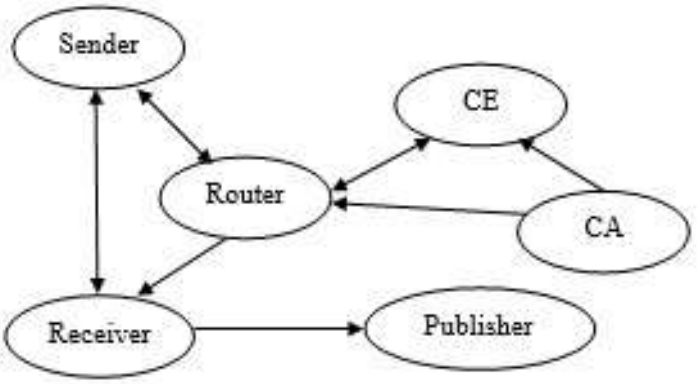
SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 12 | December 2024 - Peer Reviewed Journal

1.3. EXISTING SYSTEM

Existing big data retrieval models struggle with inefficiencies and vulnerabilities, especially in unpredictable environments. Traditional authentication systems, which rely heavily on centralized servers, fail to address critical security concerns such as malicious-request and data-poisoning attacks. Moreover, centralized systems often suffer from increased latency and lack scalability, making them inadequate for modern decentralized networks. This research aims to overcome these limitations by proposing a data-centric authentication system that enhances network resilience and security without relying on centralized resources.

Current systems in big data networks primarily rely on centralized authentication models that authenticate interactions between users and publishers. However, these systems suffer from prolonged authentication delays and vulnerabilities to various attacks, including cache poisoning and request flooding. The reliance on centralized servers increases latency and introduces single points of failure, making the system less efficient and more susceptible tobreaches.Conventional authentication systems struggle with inefficiencies in dynamic network e nvironments. Centralized authentication models introduce high latency and expose networks to attacks such as cache poisoning and request flooding. Additionally, existing models fail to ensure privacy and scalability in handling large-scale data retrievals. This paper proposes a data-centric authentication model to address these challenges, enhancing both security and performance.

1.3.1 SYSTEM ARCHITECTURE



EXPLANATION

The proposed system architecture incorporates a suspension-chain model that integrates CA-based and neighbor-based trust for seamless authentication. This architecture ensures real-time validation of data and users, significantly reducing the risk of malicious activities. By embedding authentication processes into data forwarding mechanisms, the system minimizes delays and enhances security across various network nodes.

The proposed DC Auth System Architecture introduces a distributed trust model using Suspension Certificate Chains. The architecture consists of:

User Module: Generates and forwards data requests.
Router Module: Validates certificates using suspension chains.
Publisher Module: Authenticates and provides data securely.
Certificate Authority (CA): Issues and manages certificates for network entities.
The system ensures real-time validation through hop-by-hop trust verification, significantly reducing delays

The DC Auth system employs a multi-layered approach involving data caching, trust verification, and secure packet forwarding. The suspension-chain model enables dynamic trust establishment between network entities, ensuring continuous authentication without centralized dependency. The trust chain is established through certificates exchanged between neighboring entities, significantly reducing authentication time and enhancing overall system performance.

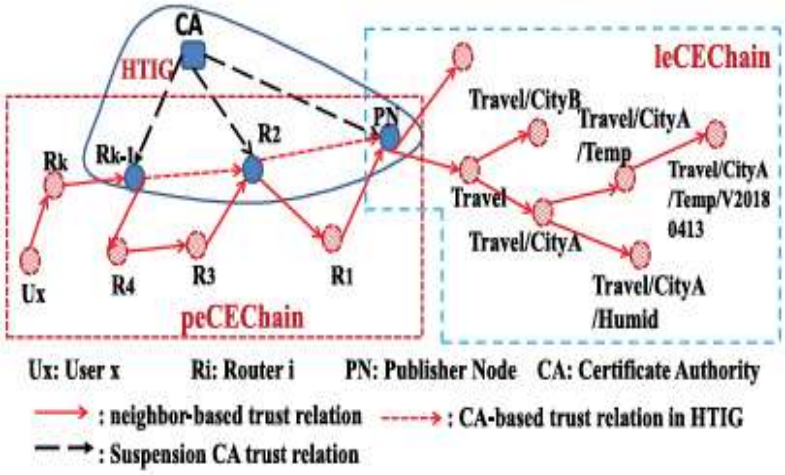
1.3.2 EXISTING SYSTEM DISADVANTAGES

High Latency: Centralized authentication processes significantly increases delays
Vulnerability to Attacks: Susceptible to malicious-request and data-poisoning attacks.
Limited Scalability: Heavy reliance on centralized servers restricts system scalability.

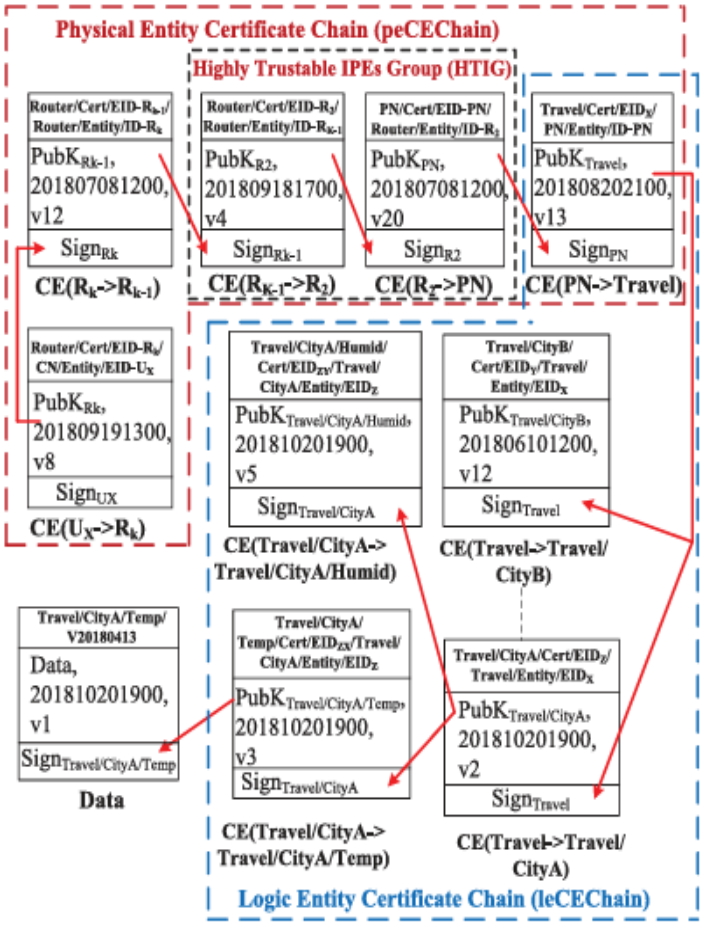
SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 12 | December 2024 - Peer Reviewed Journal

1.4 PROPOSED SYSTEM

The DC Auth model introduces a novel approach to secure big data retrieval in ICN environments. By integrating CA-based and neighbor-based trust, DC Auth creates a robust suspension-chain that seamlessly authenticates users, IPEs, and publishers. Unlike traditional models, DC Auth embeds authentication within the data transmission process, enabling real-time validation without relying on central servers, thereby enhancing security and reducing latency.



(a) Trust Relation



(b) Suspension certificate chain

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 12 | December 2024 - Peer Reviewed Journal

1.4.1 PROPOSED SYSTEM ADVANTAGES

Enhanced Security: Protection against malicious-request and data-poisoning attacks.
Low Latency: Decentralized certificate management minimizes authentication delays.
Scalability: Seamless integration into ICN frameworks ensures adaptability for large-scale networks.

DESCRIPTION GENERAL

DC Auth leverages ICN principles to create a secure and efficient environment for big data retrieval. By embedding authentication into data packets, the system ensures that all data exchanges are verified for authenticity and integrity, reducing the risk of unauthorized data access or tampering.

2.METHODOLOGIES

2.1 MODULES NAME

User Interface Design
User Module
Router Module
Certificate Authority Module
Publisher Module

User Interface Design
Enables users to authenticate and interactwith the system securely.

Router Module
Facilitates certificate exchange and manages secure routing .

Certificate Authority Module
Issues and verifies certificates for network entities.

Publisher Module
Ensures data authenticity and integrity before distribution.

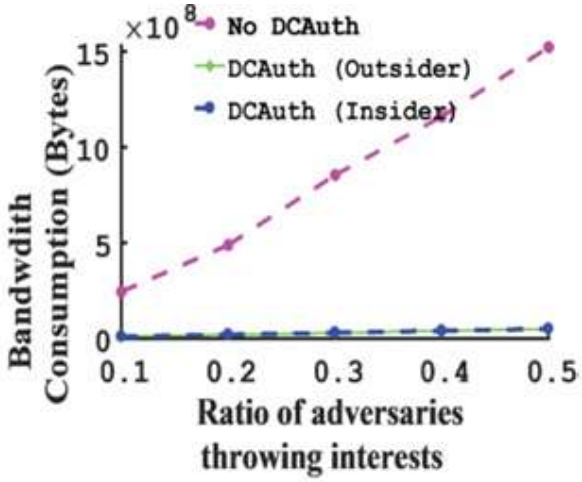
2.2 TECHNIQUES USED

The system utilizes the DC Auth Algorithm, which incorporates trust chains and data-centric authentication. By leveraging neighbor-based and CA-based trust models, DC Auth ensures secure communication across all network layers, mitigating the risks associated with malicious data exchanges and unauthorized access.

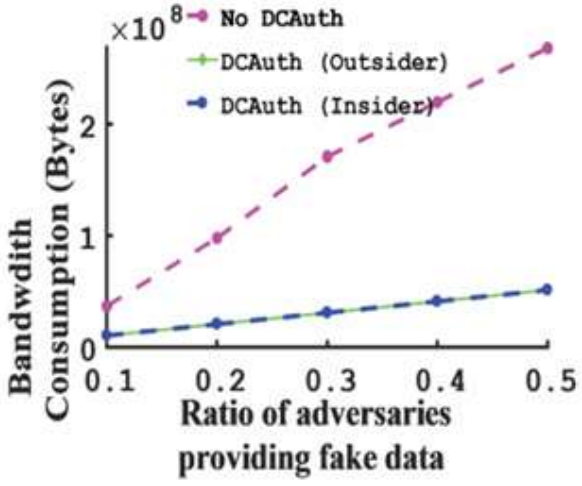
3.RESULT

Simulations of the DC Auth model demonstrate significant improvements in network security and performance. The system achieves a high accuracy rate in detecting and mitigating attacks, significantly reducing latency compared to traditional authentication methods. Extensive testing indicates that DC Auth not only enhances data integrity but also ensures faster, more secure data retrieval in ICN environments.

SJIF Impact Factor (2024): 8.675| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 9 | Issue: 12 | December 2024 - Peer Reviewed Journal



Bandwidth consumption under Interest flooding attack.



Bandwidth consumption under fake data attack.

4. FUTURE ENHANCEMENT

Future enhancements of DC Auth will focus on integrating advanced machine learning algorithms to dynamically detect and respond to emerging threats. Additionally, incorporating biometric authentication and blockchain technology could further strengthen the system's security. Expanding the framework to include IoT-specific protocols will enhance its applicability in diverse, large-scale environments, setting new standards in secure network communication.

5.CONCLUSION

In-network big data retrieval is inherently vulnerable to security risks such as malicious requests and data-poisoning attacks. The proposed DC Auth model addresses these challenges by providing a robust, data-centric authentication mechanism that combines CA-based and neighbor-based trust. By integrating authentication into the data forwarding process, DC Auth significantly reduces latency and enhances security, making it a scalable and efficient solution for modern ICN environments.

6. REFERENCES

1. *Khan, I. Yaqoob, et al., "Big Data: Survey, Technologies, Opportunities, and Challenges," The Scientific World Journal, 2014.*
2. *Yin, H., Jiang, Y., et al., "Big data: Transforming the design philosophy of future Internet," IEEE Network, 2014.*
3. *Saltzer, J., Reed, D., and Clark, D., "End-to-end arguments in system design," ACM Transactions on Computer Systems, 1984.*
4. *Yu, S., and Guo, S., "Networking for Big Data: A Survey," IEEE Communications Surveys and Tutorials, 2017. AbduAllah, E., Hassanein, H., "A survey of security attacks in information-centric networking," IEEE Communications Surveys & Tutorials, 2015.*
5. *Gasti, P., Tzadik, G., "DoS and DDoS in named data networking," IEEE ICCCN, 2013.*