Data access control for named data of health things

Asmaa EL-Bakkouchi[1], Mohammed EL Ghazi[1], Anas Bouayad[1], Mohammed Fattah[2], Moulhime EL Bekkali[1]

[1]Artificial Intelligence, Data Sciences and Emerging Systems Laboratory, Faculty of Science and Technology, Sidi Mohamed Ben Abdellah University, Fez, Morocco
[2]IMAGE Laboratory, Moulay Ismail University, Meknes, Morocco

Article Info

Article history:

Received Mar 14, 2023
Revised Nov 28, 2023
Accepted Feb 12, 2024

Keywords:

Access control
Internet of health things
Internet of things
Named data networking
Named data of health things

ABSTRACT

The internet of health things (IoHT) represents an innovative network concept that significantly improving healthcare. However, security and privacy are the main concerns of IoHT because the transmitted health data is often sensitive data about patients' health status, which needs to be secured and protected from unauthorized users and any leakage. Named data networking (NDN) is considered the most promising architecture for the future internet that perfectly fits with the requirements of IoHT systems, especially regarding security and privacy. In this paper, we exploit the fundamental features of NDN to design a robust system for IoHT to ensure secure communication and access to health data. This system presents a content access control model, which prevents attackers and unauthorized users from accessing health data, allows only authorized users to access these data, and prevents users from accessing "corrupted" or "fake" content. The simulation results show that the proposed mechanism slightly delays the secure retrieval of health data. However, this delay is tolerable since the mechanism protects the health data from unauthorized persons and those who try to inject untrusted data into the network.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Asmaa EL-Bakkouchi
Artificial Intelligence, Data Sciences and Emerging Systems Laboratory
Faculty of Science and Technology, Sidi Mohamed Ben Abdellah University
Fez, Morocco
Email: asmaa.elbakkouchi@usmba.ac.ma

1. INTRODUCTION

The internet of health things (IoHT) is an extended version of the internet of things (IoT) [1], [2] that refers to a collection of internet-connected devices used to carry out tasks and provide healthcare support services [3] by enabling the collection, processing, transfer, and tracking of patient health data through IoT devices and sensors [4]. IoHT has demonstrated enormous promise to make the healthcare field smart through IoT applications and devices that aim to improve treatments, decrease defects, control diseases, and lower costs [5]. However, several healthcare-related elements are bringing new approaches and aggressive challenges to the healthcare infrastructure that need to be studied and improved.

Our study addresses two identified data access challenges in the context of health data sharing between healthcare staff and patients. Firstly, as healthcare data often contains susceptible information about a patient's health status [6], it should only be accessible to authorized users. Currently, this access control is carried out manually or using passwords, resulting in high overheads and being prone to human error. Secondly, personal information and sensitive patient data could be altered, used, or compromised without real-time control. This poses a risk to the infrastructure and a disastrous effect on people's lives, as the transmission of false data can lead to misdiagnosis and severe health problems and even put patients' lives at risk [7], [8]. If these data can be verified (data authentication), this prevents users from accessing erroneous or falsified data.

To meet the above challenges, we rely on the functionalities provided by named data networking (NDN) [9]-[12] (which represents the most suitable information-centric networking (ICN) [13] architecture for IoHT [14]), including name-based access control to manage data access. Our contribution consists of a content access control model that firstly prevents unauthorized users and attackers from accessing protected healthcare data and allows only authorized users to access these data. Secondly, it prevents healthcare users from accessing erroneous or falsified data. This model allows each node to control the data it receives without having to notify another node to do so, which is advantageous in terms of optimizing data recovery time, unlike the majority of existing NDN access control solutions, which, despite their advantages, require additional interaction with specific nodes to ensure data access control, resulting in increased data retrieval time, which is a critical point in the healthcare field.

The paper is structured as follows. In section 2, we briefly present related work, then in section 3, we describe the proposed mechanism, and in section 4, we evaluate the performance of the proposed mechanism by presenting the simulation parameters and discussing the obtained results. Finally, we conclude the paper and future work in section 5.

2. RELATED WORK

Nowadays, IoHT has emerged as a promising new technology to make the healthcare field smart [15]. It enables the collection, processing, transfer, and monitoring of health data remotely using IoT devices and sensors [14]. These data are often sensitive patient data that require high protection against any risk of leakage or loss [16]. Hence, access control is essential for the security of these data and to prohibit unauthorized users from accessing the protected data.

To achieve effective access control and protect data privacy, EPB-ACM has been proposed in [17]. According to this mechanism, the producer encrypts the content using a symmetric key, and the content key is encrypted using the authorized user’s public key. After obtaining the encrypted content, the authorized user should contact the producer for the decryption key. Despite the advantages of this concept in solving the replica content problem, additional interaction between the user and the producer is required to obtain the decryption key, resulting in losing the NDN’s advantage in terms of content recovery time. Similarly, the works in [18]–[20] also use content encryption by a key and, therefore, have the same disadvantage of needing additional interaction with the producer or the management center to request the decryption key. Feng and Guo [21] used content encryption by the attribute-based key and ciphertext policy. The producer creates the access control policy to encrypt the data. The policy is then sent as ciphertext over the network, and the attribute values are cached. The consumer must always ask the multiattribute authorities for the key because the ciphertext can only be decrypted if its attributes fit the access structure. Mamane *et al.* [22] propose using hash-based and encryption-based name obfuscation to control content access by preventing unauthorized users from obtaining the content. However, name obfuscation leads to the creation of multiple replicas of the same content, significantly reducing network caching efficiency.

Additionally, the producer must calculate the hashed content names in advance for each user and keep a table that maps the real name to the obfuscated name when using hash-based obfuscation, which adds computation and storage expenses. Wu *et al.* [23] proposed an access control mechanism based on attributes and an encryption policy. In this mechanism, the producer divides the content request into two sections: the content named the public content section (PCS), the second concerns the key, and the consumers named the content key section (CKS). The principal drawback of this mechanism is the need for additional interaction between the consumer and the producer to obtain the decryption key, which increases the content retrieval time and requires that the producer is available (connected), which is not always the case. Li *et al.* [24] proposed an attribute-based encryption naming scheme to manage the attributes of the content in a distributive manner using an ontology-based management system and to apply the access rules to public or cacheable routers using a name attribute collection. Its primary disadvantage is that it only applies to flat naming schemes and cannot be applied to hierarchical ones.

Based on the above research work, despite many approaches that have been proposed, the achievability of access control in an NDN network is still limited by some problems. Content key encryption is undoubtedly the principal mechanism used for access control. However, the major problem that needs to be solved is the optimization of the content retrieval time, which limits the network’s performance, especially for domains in which the data retrieval time is significant, like IoHT, and as the data exchanged in IoHT are sensitive data that require a low delay. We propose an access control mechanism for health data that adds an access value to the interest packet to prevent unauthorized users from accessing these data and also adds a trust value to the data packet to prevent users from accessing erroneous or false data.

3. THE PROPOSED MECHANISM

In IoHT, healthcare applications transmit and receive health data between each other and with healthcare personnel in open-access environments such as the NDN architecture, which has no restrictions on who may access what type of data. These health data often contain susceptible data about the health status of patients [6], which need to be secured and protected from unauthorized users due to their critical nature. However, IoT has a pervasive nature where the risks of security and privacy breaches are very high if the automatic data collection is not verified and managed correctly. Patients' personal information and sensitive data could be altered, utilized, or compromised without real-time control. This not only constitutes a risk to infrastructure but also has a disastrous effect on people's lives, as the transmission of false data can result in misdiagnosis and severe health problems and even put patients' lives in danger [7]. Therefore, an access control mechanism is needed to protect health data from being leaked or lost and from unauthorized users. Access control constitutes an important security aspect in IoHT environments. Without access control, it is impossible to distinguish between legitimate and malicious entities; data producers may publish their data under any namespace, and users may access any content, which is exceptionally undesirable in IoHT because of the sensitivity of transmitted data.

3.1. Mechanism objectives

Our objective is to limit access to available content, prevent unauthorized users from accessing health data, allow only authorized users to access these data, and prevent users from accessing "corrupted" or "fake" content. This is done by:

- Verifying the integrity and authenticity of users requesting health data.
- Enforcing an access control policy to prevent attackers and unauthorized users from accessing health data.
- Verifying the integrity and authenticity of the data received to prevent users from accessing "corrupted" or "false" content.

3.2. Mechanism overview

Our new mechanism consists of preventing attackers and unauthorized users from accessing protected health data and preventing authorized users from accessing "corrupted" or "false" data. The existing system has been modified by adding a new field in the interest packet, a new field in the data packet, a new table at the content producer concerning access information, and a new table at the user containing the trust values of each health service.

This model works as follows: the user (consumer) sends an interest packet with the access value, and then the router checks if this packet contains an access value or not to transmit it to the content producer. If the received interest packet contains an access value, it transmits it to the producer. Otherwise, it deletes it and considers that the user cannot access the health data. Once the producer receives this packet, it extracts the access value to compare it with the values available in its access control table to decide whether the user is authorized to receive the content he requested or not. Based on this comparison, the producer decides whether to send the requested content. If the extracted access value matches one of the values available in its table, the producer sends the corresponding data packet. Otherwise, it deletes the interest packet. Once it receives a data packet, it extracts the trust value and compares it to its table. If the trust value is available in its table, the user accepts the data packet; otherwise, it deletes it and considers it untrusted.

3.3. Mechanism design

Figure 1 presents the secured model for IoHT in NDN networks. This model contains a user, a router, and a content producer and relies on a three-step access control: a control at the router for filtering interest packets, a control at the producer for limiting access to protected health data, and a control at the user for distinguishing trusted data from erroneous and fake data. To start a secure communication, the user adds an access value to the header of the interest packet to request the health data and sends this packet to the router, which is charged to forward it to the content producer.

The NDN router plays an essential role in this communication, and it selects the packets to be forwarded to the producer, i.e., it filters the packets to be forwarded by forwarding only the packets that contain an access value. The router does not know the access values that are valid to receive the health data, and its role is to filter the packets that do not contain access values.

On the router side, if the interest packet received contains an access value, it forwards it to the producer. Otherwise, it deletes this packet and considers that the user cannot access the health data. On the producer side, when it receives an interest packet, it extracts the access value to check whether the user is authorized to receive the corresponding health data. If the access value matches one of its authorized access table values, the producer adds a trust value to the header of the corresponding data packet and sends it to the user. Otherwise, it deletes the interest packet and considers that the user cannot access the health data. On the user side, when it receives a data packet, it first checks whether it contains a trust value. If it does not contain a trust value, it directly deletes this packet; otherwise, it extracts the trust value and checks if it is available in its trust list to ensure the authenticity of the received data; otherwise, it deletes this packet.

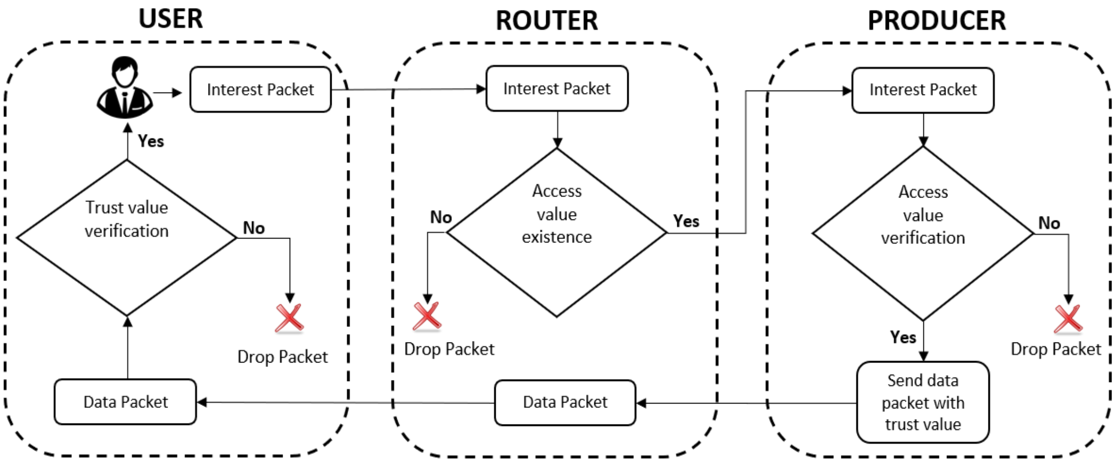


Figure 1. Proposed mechanism scheme

3.4. The proposed algorithms

Algorithm 1 illustrates the interest packet filtering algorithm at the intermediate router. In this algorithm, the router uses an access-value-based filter, i.e., when it receives an interest packet, it checks whether or not it contains an access value. If the interest packet contains an access value, the router forwards it to the producer; otherwise, it discards it.

Algorithm 1. Router interest filtering algorithm

```
function ONINTEREST (InterestPacket)
  if (interest packet contains an access value) then
          send this packet to the producer;
  else
          drop this packet;
  end if
end function
```

Algorithm 2 illustrates the accessibility verification algorithm executed by the content producer. First, the producer extracts the access value from the header of the interest packet and checks if this access value is included in its table of authorized accesses to obtain the health data to decide whether or not to allow the user to obtain the desired data.

Algorithm 2. Producer access verification algorithm

```
function ONINTEREST (InterestPacket)
  Accessvalue ← GetAccessValue (InterestPacket);
  // Verification if Access Value is available in its access table
  if (Accessvalue == True) then
          add trust value to the corresponding data packet;
          send this data packet to the user;
  else
          drop interest packet;
  end if
end function
```

Algorithm 3 illustrates the algorithm for validating the received data at the user. In this algorithm, when the user receives a data packet, he first checks the existence of the trust value and then ensures that it is available in its trust list to guarantee the authenticity of the data received. Otherwise, if the data packet does not contain a trust value, the user directly deletes it.

Algorithm 3. Consumer data validation algorithm

```
function ONDATA (DataPacket)
  // Verification if data packet contains a trust value
```

```
    if (data packet contains a Trust Value) then
        TrustValue ← GetTrustValue (DataPacket);
        // Verification if trust value is available in its trust list
        if (TrustValue == True) then
            get the data packet;
        else
            drop the data packet;
        end if
    else
        drop the data packet;
    end if
end function
```

4. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the proposed NDN-based IoHT mechanism in different scenarios. We use the ndnSIM simulator [25] to implement the proposed mechanism and the C++ language to write the programs. We are mainly interested in the data retrieval time, which is defined as the elapsed time between the sending of an interest packet by a user and the receiving of the corresponding data packet, including the time to verify the authenticity and privacy of the users and producers of the data, and we measure this time for different numbers of requests per second and the use of multiple routers (for communication overhead).

4.1. Simulation environment and parameters

In named data of health things (NDoHT), access delay constitutes a critical issue because every demand gets one response, and without a demand, no response can exist, unlike non-name-based architectures where requests are likely to receive multiple data packets. This implies that security measures must be applied to each request. We aim to achieve optimal access delay results while reducing the necessary overhead.

In our experiments, the first scenario aims to validate the proposed scheme scenario to limit access to health data for unauthorized users, prevent the user from accessing erroneous data, and ensure the transmission of patient health data for authorized users. It consists of three users (two authorized users and one unauthorized user), one router, and two content producers (one trusted producer and the other considered fake or attacker). The link rate in this scenario is 1 Mbps with a latency of 10 ms. We employ the best route transfer strategy and transfer a health data file of size 1024 bytes. In this scenario, each user sends one request per second for the 50 s.

In the second scenario, we use a topology that contains 20 users, 5 routers, and 4 producers. Every 5 users request data from a producer, with a link rate of 1 Mbps and a latency of 10 ms. We employ the best route transfer strategy and transfer a health data file of size 1024 bytes. We evaluate the performance of the proposed mechanism and standard NDN with different numbers of requests per second ranging from 10 req/s to 1000 req/s. We compare the average data retrieval time between standard NDN and the proposed mechanism. Standard NDN's average data retrieval time is measured in the normal case without access control.

Finally, we study the impact of overhead in communication on the user side's retrieval time of health data. For this, we use a topology that consists of one user and one producer, and with each simulation, we increase the number of routers from 1 to 8. The link rate in this scenario is 10 Mbps with a latency of 10 ms. We employ the best route forwarding strategy, and the user requests one health data per second with a size of 1024 bytes. We apply the interest packet filtering algorithm only at the first router.

4.2. Results and discussions

Figure 2 illustrates the data retrieval time of the first scenario. In this figure, the authorized user (user 1) retrieved the requested health data with an average delay of 49 ms between sending the request and retrieving the corresponding packet, including the time to verify the authenticity and privacy of the users and producers of the data. For user 2, the delay is zero since he is not authorized to access the protected data, so the producer had to delete his request and send a message to this user to inform him that he is not authorized to access the data. Similarly, for user 3, since the data that arrived does not contain a trust value, the user has deleted it. This data is received, and the delay is considered zero since no request has been satisfied. Figure 3 illustrates an example of Figure 3(a) a message received by the unauthorized user in response to his data request and Figure 3(b) a message received by the untrusted producer from user 3 to inform him that he is not a trusted producer.

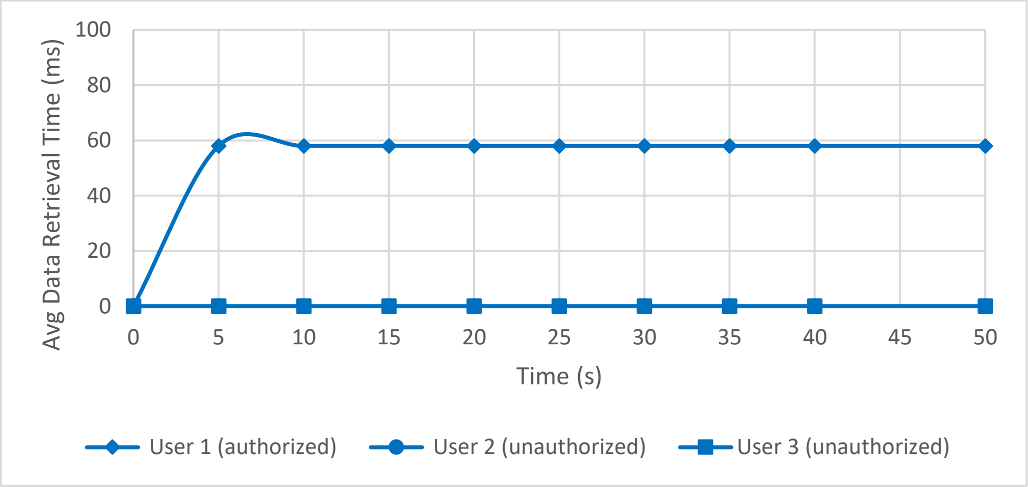
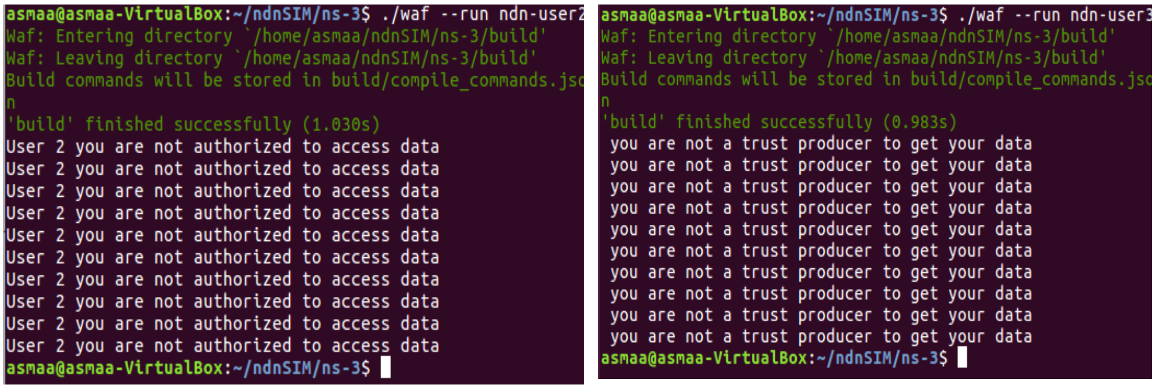


Figure 2. Average data retrieval delay of scenario 1



```
asmaa@asmaa-VirtualBox:~/ndnSIM/ns-3$ ./waf --run ndn-user2
Waf: Entering directory `/home/asmaa/ndnSIM/ns-3/build'
Waf: Leaving directory `/home/asmaa/ndnSIM/ns-3/build'
Build commands will be stored in build/compile_commands.jsc
n
'build' finished successfully (1.030s)
User 2 you are not authorized to access data
User 2 you are not authorized to access data
User 2 you are not authorized to access data
User 2 you are not authorized to access data
User 2 you are not authorized to access data
User 2 you are not authorized to access data
User 2 you are not authorized to access data
User 2 you are not authorized to access data
User 2 you are not authorized to access data
User 2 you are not authorized to access data
asmaa@asmaa-VirtualBox:~/ndnSIM/ns-3$
```

(a)

```
asmaa@asmaa-VirtualBox:~/ndnSIM/ns-3$ ./waf --run ndn-user3
Waf: Entering directory `/home/asmaa/ndnSIM/ns-3/build'
Waf: Leaving directory `/home/asmaa/ndnSIM/ns-3/build'
Build commands will be stored in build/compile_commands.jsc
n
'build' finished successfully (0.983s)
 you are not a trust producer to get your data
 you are not a trust producer to get your data
 you are not a trust producer to get your data
 you are not a trust producer to get your data
 you are not a trust producer to get your data
 you are not a trust producer to get your data
 you are not a trust producer to get your data
 you are not a trust producer to get your data
 you are not a trust producer to get your data
 you are not a trust producer to get your data
asmaa@asmaa-VirtualBox:~/ndnSIM/ns-3$
```

(b)

Figure 3. Messages received by: (a) unauthorized users and (b) untrusted producers

Figure 4 shows the simulation result of the second scenario. It shows the average data retrieval time of the proposed mechanism and the NDN standard for different numbers of requests per second. The average data retrieval time is about 57 ms and 40 ms for the proposed mechanism and standard NDN, respectively, when users requested 10 req/s. These average data retrieval time values become 82 ms and 43 ms for the proposed mechanism and standard NDN, respectively, when the number of requests per second increased to 100 req/s. Similarly, for 500 req/s, the average data retrieval time is 542 ms and 57 ms, and for 1000 req/s, it is 854 ms and 376 ms for the proposed and standard NDN mechanism, respectively. We notice that the data retrieval time increases when requests increase. The reason for this is that when the user sends several requests at the same time or when several users participate in communication at the same time and send several requests at the same time, it takes more time to process each request since each request first passes through filtering at the routers before arriving at the data producer which in turn first ensures the authenticity of the user (if it is authorized or not) and then responds to each request with its corresponding data packet which requires more time than in the case of standard NDN where no access control is applied. This average data retrieval time increase is insignificant compared to the mechanism's security improvement.

Figure 5 shows the simulation result of the data retrieval time of the last scenario. We notice that with the increase in the number of routers, the data retrieval time also increases, which is explained by the fact that the data request has to pass through several routers before arriving at the producer. Similarly, for the response to this request, the data packet has to pass through several routers before arriving at the user, which consequently increases the time between sending the request and retrieving the corresponding data.

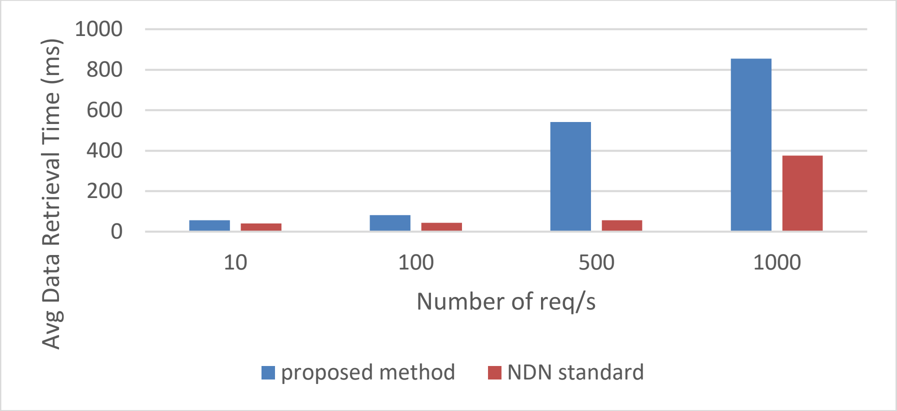


Figure 4. Average data retrieval delay of scenario 2

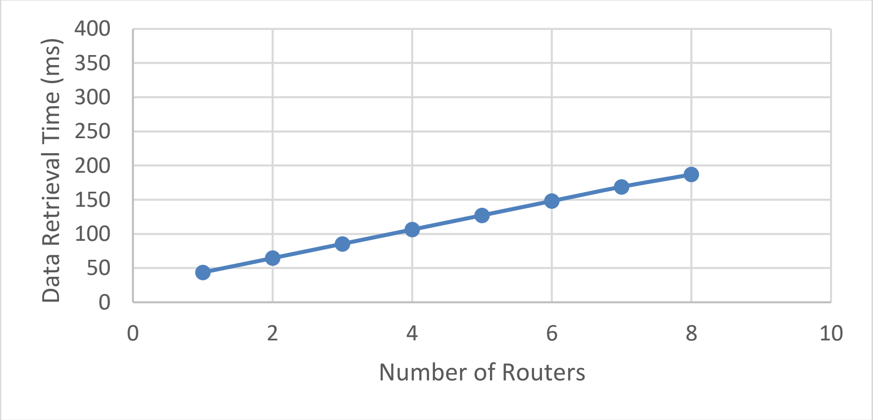


Figure 5. Data retrieval time for n routers

5. CONCLUSION

This paper proposes an NDN-based access control mechanism for IoHT to ensure secure communication and access to health data. This mechanism allows the application of security policies on access to health data. We also use this mechanism to filter requests on the router side and data received on the user side. In addition, the goal of our mechanism is to limit access to available data, prevent attackers and unauthorized users from accessing health data, and allow only authorized users to access health data, as well as prevent users from accessing "corrupted" or "fake" data. We implemented and evaluated our mechanism in the ndnSIM simulator. The results of our simulations prove the effectiveness of our mechanism. In future work, we plan to examine the privacy and security issues of cached content.

REFERENCES

[1] M. O. Rahaman *et al.*, "Internet of things based electrocardiogram monitoring system using machine learning algorithm," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 4, pp. 3739–3751, Aug. 2022, doi: 10.11591/ijece.v12i4.pp3739-3751.

[2] R. Boussada, B. Hamdane, M. E. Elhdhili and L. A. Saidane, "PP-NDNoT: On preserving privacy in IoT-based E-health systems over NDN," *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, Marrakesh, Morocco, 2019, pp. 1-6, doi: 10.1109/WCNC.2019.8886110.

[3] D. Saxena, V. Raychoudhury, and N. SriMahathi, "SmartHealth-NDNoT," in *Proceedings of the 2015 Workshop on Pervasive Wireless Healthcare*, Jun. 2015, pp. 45–50, doi: 10.1145/2757290.2757300.

[4] Aroosa, S. S. Ullah, S. Hussain, R. Alroobaea, and I. Ali, "Securing NDN-Based Internet of Health Things through Cost-Effective Signcryption Scheme," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–13, Apr. 2021, doi: 10.1155/2021/5569365.

[5] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment," in *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*, Oct. 2017, pp. 112–120, doi: 10.1109/LCN.Workshops.2017.72.

[6] A. El-Bakkouchi, M. El Ghazi, A. Bouayad, M. Fattah, and M. El Bekkali, “Hybrid Congestion Control Mechanism as a Secured Communication Technology for the Internet of Health Things,” in *Artificial Intelligence and Smart Environment*, Cham: Springer, 2023, pp. 498–503, doi: 10.1007/978-3-031-26254-8_72.

[7] A. A. Rezaee, M. H. Yaghmaee, A. M. Rahmani, and A. H. Mohajerzadeh, “HOCA: Healthcare Aware Optimized Congestion Avoidance and control protocol for wireless sensor networks,” *Journal of Network and Computer Applications*, vol. 37, pp. 216–228, Jan. 2014, doi: 10.1016/j.jnca.2013.02.014.

[8] J. Karande and S. Joshi, “DEDA: An algorithm for early detection of topology attacks in the internet of things,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 2, pp. 1761–1770, Apr. 2021, doi: 10.11591/ijece.v11i2.pp1761-1770.

[9] L. Zhang *et al.*, “Named Data Networking (NDN) Project Named Data Networking (NDN) Project,” 2010.

[10] M. N. O. Sadiku, A. E. Shadare, and S. M. Musa, “Named data networking,” *International Journal of Engineering Research*, vol. 6, no. 7, pp. 371–372, 2017, doi: 10.5958/2319-6890.2017.00040.X.

[11] A. EL-Bakkouchi, A. Bouayad, and M. EL Bekkali, “A hop-by-hop Congestion Control Mechanisms in NDN Networks – A Survey,” in *2019 7th Mediterranean Congress of Telecommunications (CMT)*, Oct. 2019, pp. 1–4, doi: 10.1109/CMT.2019.8931405.

[12] A. El-Bakkouchi, M. El Ghazi, A. Bouayad, M. Fattah, and M. El Bekkali, “EC-Elastic an Explicit Congestion Control Mechanism for Named Data Networking,” *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 11, pp. 594–603, 2021, doi: 10.14569/IJACSA.2021.0121168.

[13] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, “A survey of information-centric networking,” *IEEE Communications Magazine*, vol. 50, no. 7, pp. 26–36, Jul. 2012, doi: 10.1109/MCOM.2012.6231276.

[14] A. El-Bakkouchi, M. El Ghazi, A. Bouayad, M. Fattah, and M. El Bekkali, “Average Delay-based early Congestion Detection in Named Data of Health Things,” *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 7, pp. 335–342, 2022, doi: 10.14569/IJACSA.2022.0130742.

[15] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and Kyung-Sup Kwak, “The Internet of Things for Health Care: A Comprehensive Survey,” *IEEE Access*, vol. 3, pp. 678–708, 2015, doi: 10.1109/ACCESS.2015.2437951.

[16] H. H. Hlaing, Y. Funamoto, and M. Mambo, “Secure Content Distribution with Access Control Enforcement in Named Data Networking,” *Sensors*, vol. 21, no. 13, p. 4477, Jun. 2021, doi: 10.3390/s21134477.

[17] T. Chen, K. Lei, and K. Xu, “An encryption and probability based access control model for named data networking,” in *2014 IEEE 33rd International Performance Computing and Communications Conference (IPCCC)*, Dec. 2014, pp. 1–8, doi: 10.1109/PCCC.2014.7017100.

[18] S. K. Ramani, R. Tourani, G. Torres, S. Misra, and A. Afanasyev, “Ndn-abs: Attribute-based signature scheme for named data networking,” in *Proceedings of the 6th ACM Conference on Information-Centric Networking*, Sep. 2019, pp. 123–133, doi: 10.1145/3357150.3357393.

[19] Q. Li, X. Zhang, Q. Zheng, R. Sandhu, and X. Fu, “LIVE: Lightweight Integrity Verification and Content Access Control for Named Data Networking,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 308–320, Feb. 2015, doi: 10.1109/TIFS.2014.2365742.

[20] B. Hamdane and S. G. El Fatmi, “A credential and encryption based access control solution for named data networking,” in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, May 2015, pp. 1234–1237, doi: 10.1109/INM.2015.7140473.

[21] T. Feng and J. Guo, “A New Access Control System Based on CP-ABE in Named Data Networking,” *International Journal of Network Security*, vol. 20, no. 4, p. 13, 2018.

[22] A. Mamane, M. El Ghazi, S. Mazer, M. Bekkali, M. Fattah, and M. Mahfoudi, “The impact of scheduling algorithms for real-time traffic in the 5G femto-cells network,” in *2018 9th International Symposium on Signal, Image, Video and Communications (ISIVC)*, Nov. 2018, pp. 147–151, doi: 10.1109/ISIVC.2018.8709175.

[23] Z. Wu, E. Xu, L. Liu, and M. Yue, “CHTDS: A CP-ABE access control scheme based on hash table and data segmentation in NDN,” in *Proceedings - 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering, TrustCom/BigDataSE 2019*, 2019, pp. 843–848, doi: 10.1109/TrustCom/BigDataSE.2019.00122.

[24] B. Li, D. Huang, Z. Wang, and Y. Zhu, “Attribute-based Access Control for ICN Naming Scheme,” *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 2, pp. 194–206, Mar. 2018, doi: 10.1109/TDSC.2016.2550437.

[25] S. Mastorakis, A. Afanasyev, I. Moiseenko, and L. Zhang, “ndnSIM 2 . 0 : A new version of the NDN simulator for NS-3,” in *NDN Project*, 2015, pp. 1–8.

BIOGRAPHIES OF AUTHORS

Asmaa EL-Bakkouchi is currently pursuing a Ph.D. in the Artificial Intelligence, Data Science, and Emerging Systems Laboratory at Sidi Mohamed Ben Abdellah University, Fez, Morocco. She obtained a Bachelor’s degree in Electronics, Telecommunications, and Computer Science (2013) from the Faculty of Science and Technology, Sidi Mohamed Ben Abdellah University, Fes, Morocco, and a Master’s degree in Telecommunication Systems Engineering (2015) from the Faculty of Science, Abdelmalek Essaadi University, Tetouan, Morocco. Her research interests include named data networking (NDN), congestion control, access control, and internet of health things (IoHT). She can be contacted at email: asmaa.elbakkouchi@usmba.ac.ma.

Mohammed EL Ghazi is a professor at the Superior School of Technology, Department of Electrical and Computer Engineering, Sidi Mohamed Ben Abdellah University (USMBA), Fez, Morocco. He received his Ph.D. at the University of Le Havre, France. He is a Laboratory of Artificial Intelligence, Data Sciences and Emerging Systems (LIASSE) member. His research focuses on BAN and new-generation networks (V2X, SDN, NDN, 5G, virtualization and cloud, 5G). He can be contacted at email: mohammed.elghazi@usmba.ac.ma.

Anas Bouayad is a Professor at Dhar El Mahraz Faculty of Sciences, Sidi Mohamed Ben Abdellah University (USMBA), Fez, Morocco. He obtained his Network and Telecommunications Engineer diploma from the National School of Applied Sciences of Fez in 2010. Further, he got his Ph.D. in Computer Sciences in 2016 from the "University Sidi Mohamed Ben Abdellah" of Fez. His research interests include cloud security, wireless body area networks (WBAN), named data networks, congestion control in NDN, and IoT4D. He can be contacted at email: anas.bouayad@usmba.ac.ma.

Mohammed Fattah received his Ph.D. in Telecommunications and CEM at the University of Sidi Mohamed Ben Abdellah (USMBA) Fez, Morocco, 2011. He is a professor in the Electrical Engineering Department of the High School of Technology at the Moulay Ismail University (UMI), Meknes, Morocco, and he is responsible for the research team 'Intelligent Systems, Networks and Telecommunications', IMAGE laboratory, UMI. He can be contacted at email: m.fattah@umi.ac.ma.

Moulhime EL Bekkali holder of a doctorate in 1991 from the USTL University - Lille 1- France, worked on printed antennas and their applications to microwave radar. Since 1992, he has been a professor at the Graduate School of Technology, Fez (ESTF) and a Transmission and Data Processing Laboratory (LTTI) member. In 1999, he received a second doctorate in electromagnetic compatibility from Sidi Mohamed Ben Abdellah University (USMBA). Currently, he works in the telecommunication domain. He is a professor at the National School of Applied Sciences (ENSAF) and a member of the LIASSE Laboratory at Sidi Mohamed Ben Abdellah University (USMBA) Fez, Morocco. He can be contacted at email: moulhime.elbekkali@usmba.ac.ma.