

Enhancing security mechanisms for robot-fog computing networks

Abdlehak Sakhi, Salah-Eddine Mansour, Abderrahim Sekkaki

Electrical and Industrial Engineering Information Processing IT and logistics (GEIL), Faculty of Sciences Ain Chock, Hassan II University, Casablanca, Morocco

Article Info

Article history:

Received Nov 27, 2023

Revised Dec 21, 2023

Accepted Jan 3, 2024

Keywords:

Cloud computing

Fog computing

Hash

HMAC

Internet of things

ABSTRACT

The evolution from conventional Internet usage to the internet of things (IoT) is reshaping communication norms significantly. Cloud computing, while prevalent, faces challenges like limited capacity, high latency, and network failures, especially when handling connected objects, leading to the emergence of fog computing as a more suitable approach for IoT. However, establishing secure connections among heterogeneous IoT entities is complex due to resource disparities and the unsuitability of existing security protocols for resource-constrained devices. This article explores fog computing's architecture, drawing comparisons with cloud computing while emphasizing its significance within the realm of IoT. Moreover, it delves into the practical application of fog computing within the context of the robot teacher project. Subsequently, our exploration introduces an advanced mutual authentication protocol, centered around hashed message authentication code (HMAC), aimed at enhancing the security infrastructure between the robot and the fog computing server.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Salah-Eddine Mansour

Electrical and Industrial Engineering Information Processing IT and logistics (GEIL)

Faculty of Sciences Ain Chock, Hassan II University

Casablanca, Morocco

Email: 19mansour94@gmail.com

1. INTRODUCTION

In our rapidly evolving technological era, the integration of artificial intelligence and robotics is fundamentally transforming our daily lives. This convergence holds immense potential for reshaping education. This research plays a pivotal role in a larger mission dedicated to refining an advanced teacher robot that harmoniously merges AI and image processing technologies [1]. Our primary research focus revolves around securing communication between these teacher robots, considered internet of things (IoT) devices, and the fog server. This security is paramount, given that the fog computing server provides the neural network's weight values crucial for the robots in classifying emotions [2].

Since in our project, we use both IoT and fog computing; the latter two encounter security difficulties coming from the scattered nature of data processing and storage, which IoT devices at the network edge, frequently resource-constrained, transfer enormous amounts of sensitive data to fog nodes for processing [3], [4]. This decentralized architecture accentuates security problems, including data privacy and integrity during transmission, as data traverses numerous network layers. Additionally, fog nodes, functioning as middlemen between IoT devices and the cloud, become potential sites of vulnerability, requiring severe procedures to secure these nodes against unauthorized access, data breaches, and malicious attacks. Establishing robust authentication procedures, encryption protocols, and continuous monitoring

systems was critical in mitigating these security concerns and assuring the confidentiality, integrity, and availability of data transiting between IoT devices and fog computing infrastructure [5], [6].

The summary covers various authentication methods in cryptography [7]. Cipher-based message authentication code (CMAC) relies on block ciphers like advanced encryption standard (AES) for secure data processing and generates authentication tags. Galois/counter mode (GCM) combines encryption and authentication, leveraging AES for data secrecy and integrity verification, notably used in various network security protocols [8]. KMAC, based on the KECCAK function, offers flexibility in customization and finds application in diverse cryptographic tasks, including post-quantum cryptography. Poly1305, paired with a secret key, ensures message integrity and authenticity by evaluating polynomial functions, especially used with AES-GCM, prioritizing data integrity and computational efficiency. Each method presents distinct features and security strengths, catering to specific cryptographic needs in diverse applications, from network security protocols to post-quantum cryptography [9], [10].

Certainly! our contribution involves crafting a security protocol reliant on hashed message authentication code (HMAC), enabling both the fog computing node and IoT devices to authenticate themselves and ensure message integrity during their communications [11]. This protocol includes the incorporation of a comprehensive dictionary within the fog computing node. This dictionary securely stores the unique IDs and corresponding secret keys of individual IoT devices. By implementing this dictionary, we aim to fortify the security measures, ensuring the protection and isolation of data belonging to each IoT device within the Fog computing infrastructure [12], [13].

In this study, section 2 will emphasize our specific contribution, concentrating on strengthening security for fog-IoT communication through the implementation of the HMAC protocol. Subsequently, section 3 will engage in a full examination of the data gained and the performance increases arising from the HMAC adjustments. This will be followed by the conclusion, summarizing the important findings and insights acquired from this study.

2. METHOD

2.1. Fog computing architecture

The architecture of fog computing, as we see in Figure 1, involves a layered framework meant to maximize data processing, storage, and computation in close to the network edge, seeking to enhance efficiency and minimize latency [14]. At its base lay numerous edge devices comprising sensors, actuators, and IoT devices responsible for data generation and collecting at the network's peripheral. These devices operate as the initial touchpoints for information within the fog computing ecosystem.

Fog nodes form the intermediate layer, intentionally positioned closer to the edge devices compared to standard centralized cloud data centers. Serving as critical processing centers, these nodes execute applications, provide storage, and offer essential network services. Ranging from routers, switches, to specialized hardware, fog nodes are optimized to handle fog computing tasks efficiently.

Fog services and applications capitalize on the computational capability of these fog nodes. These services handle data processing, analytics, and real-time decision-making, suited to individual use cases and operational requirements [15]. The fog orchestration and management layer efficiently organizes and manages the allocation of resources inside the fog computing infrastructure. This layer handles key functions like as resource allocation, security enforcement, and constant monitoring of fog nodes and services [16]. Facilitating seamless connectivity between edge devices and fog nodes, the connectivity and networking layer guarantees effective data transfer and communication. It employs a number of technologies like edge routers, wireless networks, and protocols to promote smooth interactions.

Finally, crucial to the whole design, the security and privacy layer incorporates robust techniques such as encryption, authentication, access control, and secure communication protocols. These methods safeguard data and communications, ensuring the integrity and security of information within the fog computing environment [17], [18]. The distributed nature of fog computing optimizes data processing by bringing computational resources closer to the source, permitting faster processing, reduced latency, and better efficiency for real-time applications across numerous industries and areas.

2.2. HMAC

HMAC represents a commonly used cryptographic construct meant to validate the integrity and origin of messages, ensuring secure communication over potentially insecure channels [19]. At its core, HMAC combines a cryptographic hash function with a secret key, providing a unique fixed-size authentication tag for a given message. The algorithm operates by hashing the message using a selected hash function, generally MD5, SHA-1, or SHA-256, utilizing the secret key to construct the authentication code. This code is attached to the message or transmitted alongside it. HMAC's strength comes in its resistance to

various cryptographic attacks, thanks to the use of the secret key, which is known only to the sender and recipient, making it tough for attackers to falsify or modify messages without notice.

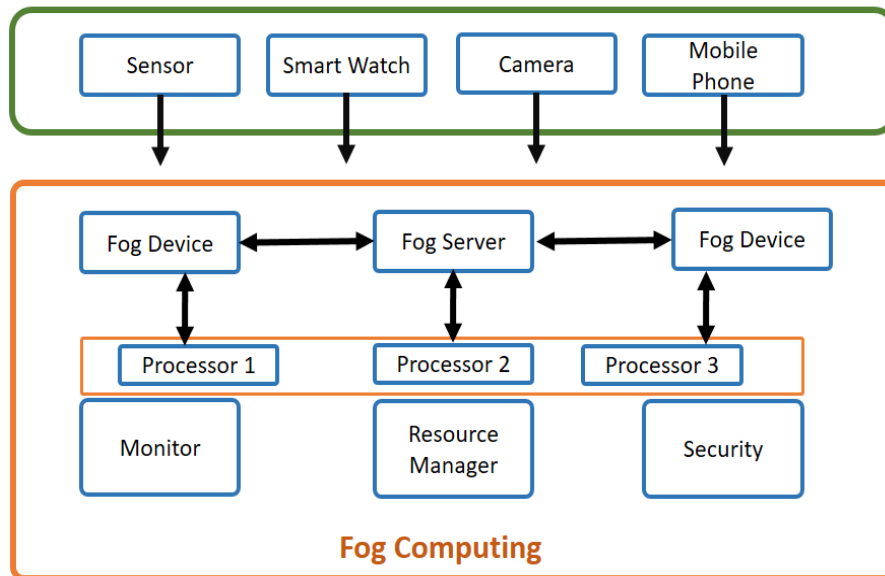


Figure 1. Fog computing architecture

One of HMAC's primary advantages is its versatility and application across multiple security protocols and systems [20]. It's extensively applied in internet security protocols like transport layer security (TLS) and internet protocol security (IPsec), where maintaining message authenticity and integrity is crucial. HMAC's ability to give high cryptographic assurance while being relatively simple to implement has made it a crucial tool in protecting communications and validating data integrity across a wide array of applications and sectors.

However, while HMAC is a powerful authentication system, its security is dependant upon various aspects. The strength of the chosen hash function directly effects the security of HMAC [21]. As processing power develops, earlier hash functions can become vulnerable to attacks, thus undermining the security of HMAC. Hence, it's necessary to frequently analyze and upgrade the hash functions used within HMAC implementations to maintain robust security against evolving threats. Additionally, key management is critical in preserving the secrecy and integrity of HMAC-protected communications, underlining the necessity for secure key storage and exchange protocols. Despite these issues, HMAC remains a cornerstone in maintaining data integrity and authenticity, playing a critical role in protecting modern digital communication networks.

2.3. IoT-fog security

In the context of an IoT-fog arrangement, the requirement of providing reciprocal authentication among networked devices looms big as a significant security concern. Given the popularity of IoT devices operating with constrained battery capacity and the requirement for frequent data transfer, the installation of a lightweight authentication mechanism becomes vital to alleviate energy consumption. In this context, we suggest a distinctive solution to authentication between a fog computing node and many IoT devices [22], [23]. Our strategy entails employing the HMAC protocol and including a compact database that serves as a dictionary holding the IDs and secret keys of each IoT device. This approach successfully segregates the data sent between the node and the devices at the hashing and security levels. The schematic representation in Figure 2 elucidates the security protocol applied between the node and the variety of IoT devices.

Prior to sending any message, the process initiates by creating a message authentication code (MAC) using a chosen hashing function like SHA256, MD5, or another specified algorithm [24], [25]. This MAC acts as a unique signature derived from the message and ensures its integrity and authenticity. It's generated by combining the message with the selected hashing function and includes an identifier, *Idi*, representing the physical address or a specific identification code associated with the IoT device generating the message. Upon transmission, the message, along with the MAC and the identifier *Idi*, is sent to its

intended destination. Upon receipt at the fog server, the transmitted components, including the identifier ID_i , are received and processed.

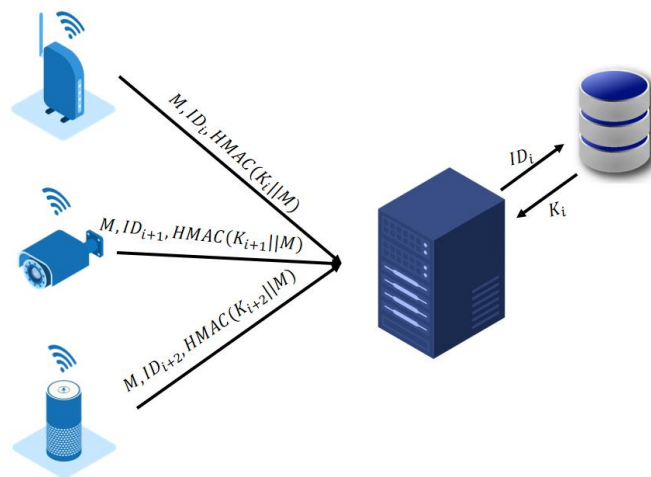


Figure 2. Communication between IoT, fog server and database

The process continues by relaying the identifier ID_i to the database to retrieve the corresponding secret key K_i associated with the specific IoT device. With the secret key K_i in hand, the same hash function used earlier (e.g., SHA256, MD5) is executed using the retrieved key and the received message [26]. This step generates a recalculated MAC', serving as a new verification code.

Subsequently, a comparison is made between the initially received MAC and the recalculated MAC'. If an exact match is found, it confirms the authenticity of the message and validates its integrity. This verification process ensures that the message has not been altered during transmission. However, any disparity between the two MACs indicates potential tampering or alterations during transit, triggering further investigation or necessary corrective actions to address the issue and maintain the integrity of the communication within the IoT infrastructure as shown in Figure 3.

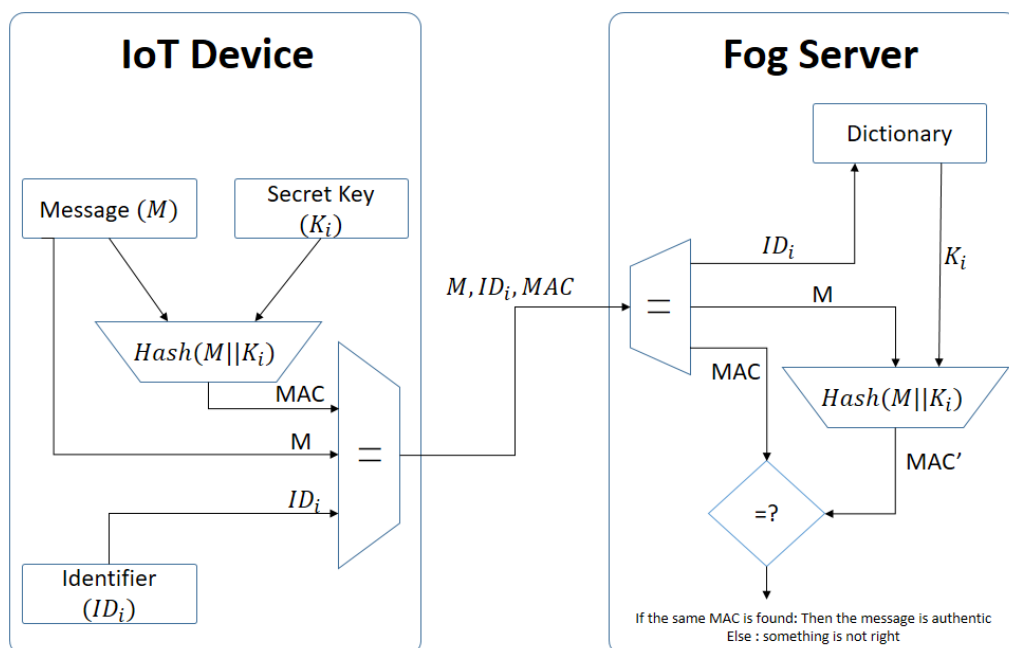


Figure 3. Verification mechanism ensuring message integrity

3. RESULTS AND DISCUSSION

The proposed protocol stands out for its exceptional efficiency, consuming minimal battery and memory resources. This makes it exceptionally suitable for constrained IoT devices. By employing the HMAC function, the protocol generates a hash using a shared secret [27]. This effectively prevents unauthorized data alterations or the creation of a new HMAC hash during transmissions. The utilization of HMAC ensures a dual layer of security, guaranteeing both the integrity and authenticity of the transmitted data.

In the present scenario, a dictionary has been introduced within the fog server, housing all the IDs paired with their respective secret keys. This measure significantly bolsters security among all IoT devices and the fog computing node. This setup ensures that even if one IoT device encounters a security breach, the remaining devices remain shielded. This heightened security is facilitated by the server's individual handling of each device through its specific secret key, thereby containing and mitigating potential risks in case of a breach on any single IoT device.

The proposed method presents a robust defense mechanism against a spectrum of security threats, ranging from replay attacks to potential man-in-the-middle breaches and clandestine attempts to intercept vital secrets. It establishes an impregnable shield, disallowing attackers from intercepting and subsequently replaying transmitted packets during the pivotal authentication and session distribution phases linking IoT Devices and the fog Node. This fortification ensures data integrity and protects against unauthorized access or manipulation.

Nevertheless, the implementation of a dictionary for elevated security measures introduces a consequential impact on response times. This deliberate decision to heighten security comes at the price of slightly diminished operational speed. However, this compromise underscores a strategic trade-off aimed at fortifying the integrity and reliability of the system's security protocols, safeguarding critical data exchanges within the IoT ecosystem.

Despite the trade-off in speed, this approach maintains its resilience and strength. It grants an elevated level of control over the accessibility of the server. This control mechanism restricts device access to services unless their unique identifiers (IDs) are specifically registered and stored within the dictionary housed in the fog node. This stringent access control paradigm ensures that only authorized devices with registered IDs can leverage and benefit from the services provided by the system. By utilizing the XOR operator to craft the MAC rather than opting for more intricate hash functions such as SHA256, MD5, or similar options, a notable reduction in the demand for extensive computational power, storage capabilities, and energy consumption is achieved. This approach streamlines the process by employing a simpler bitwise XOR operation, which results in a lighter computational load and less resource-intensive operations.

Additionally, this streamlined approach significantly curtails energy consumption. Complex hashing functions often demand intensive computational operations, consuming considerable energy, especially in resource-constrained environments like IoT devices powered by limited battery capacities. By favoring the XOR operator over resource-intensive hashing algorithms, the energy efficiency of these devices is substantially improved, leading to prolonged battery life and reduced energy overhead.

4. CONCLUSION

In the intricate intersection of IoT and fog computing, the amalgamation of these technologies brings forth intricate security challenges stemming from the decentralized nature of data processing and storage. This intricate architectural framework presents a labyrinth of hurdles, particularly concerning the confidentiality, integrity, and overall security of data as it traverses through this intricate network. In response to these intricate concerns, our comprehensive study takes center stage, introducing an innovative and resilient security protocol meticulously designed to tackle these complex issues head-on. Our protocol harnesses the robustness of HMAC to establish mutual authentication and safeguard message integrity between the myriad IoT devices and the expansive fog infrastructure. At the heart of this protocol lies a pivotal element: a dedicated dictionary meticulously housed within the fog node. This repository serves as the guardian, diligently storing and managing a catalog of unique device IDs paired with their corresponding keys. This fortified repository not only bolsters the security infrastructure but also erects impenetrable barriers, ensuring data isolation and safeguarding against unauthorized access or tampering. By fortifying this critical juncture within the network, our protocol stands as a stalwart guardian, reinforcing the very foundations of security within this intricate landscape of interconnected devices and fog computing infrastructure.




ACKNOWLEDGEMENTS

We express our deepest gratitude to the National Center for Scientific and Technical Research (CNRST) in Morocco for their indispensable support and mentorship throughout the entirety of our research journey. Their steadfast commitment to propelling scientific inquiry forward and their pivotal guidance in shaping our research direction have played an instrumental role in the successful completion of this project, perfectly in sync with the objectives of the Al-Khwarizmi Program. Their unwavering dedication has not only provided resources but also served as a beacon, illuminating our path and significantly contributing to the realization of our research aspirations. Their partnership and collaborative spirit have truly been invaluable, fostering an environment conducive to innovation and scholarly achievement.




REFERENCES

- [1] J. Nayak, K. Vakula, P. Dinesh, B. Naik, and D. Pelusi, "Intelligent food processing: Journey from artificial neural network to deep learning," *Computer Science Review*, vol. 38, p. 100297, Nov. 2020, doi: 10.1016/j.cosrev.2020.100297.
- [2] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 854–864, Dec. 2016, doi: 10.1109/JIOT.2016.2584538.
- [3] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing fog computing for internet of things applications: challenges and solutions," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 1, pp. 601–628, 2018, doi: 10.1109/COMST.2017.2762345.
- [4] L. Bittencourt *et al.*, "The internet of things, fog and cloud continuum: integration and challenges," *Internet Things*, vol. 3–4, pp. 134–155, Oct. 2018, doi: 10.1016/j.iot.2018.09.005.
- [5] M. Suárez-Albela, T. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "A practical evaluation of a high-security energy-efficient gateway for IoT fog computing applications," *Sensors*, vol. 17, no. 9, p. 1978, Aug. 2017, doi: 10.3390/s17091978.
- [6] M. Alshahrani and I. Traore, "Secure mutual authentication and automated access control for IoT smart home using cumulative Keyed-hash chain," *Journal of Information Security and Applications*, vol. 45, pp. 156–175, Apr. 2019, doi: 10.1016/j.jisa.2019.02.003.
- [7] A. Altigani, M. Abdelmagid, and B. Barry, "Analyzing the performance of the advanced encryption standard block cipher modes of operation: highlighting the National Institute of standards and technology recommendations," *Indian Journal of Science and Technology*, vol. 9, no. 28, Jul. 2016, doi: 10.17485/ijst/2016/v9i28/97795.
- [8] K. M. A. Abdellatif, "Authenticated Encryption on FPGAs from the Reconfigurable Part to the Static Part," (Doctoral dissertation, Université Pierre et Marie Curie-Paris VI), 2014.
- [9] T. Mourouzis, "Optimizations in algebraic and differential cryptanalysis," PhD diss., UCL (University College London), 2015.
- [10] J. Hiller "Improving functionality, efficiency, and trustworthiness of secure communication on an internet diversified by mobile devices and the internet of things," Auflage. Düren: Shaker, 2023.
- [11] T. W. Chim, S.-M. Yiu, V. O. K. Li, L. C. K. Hui, and J. Zhong, "PRGA: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 85–97, Jan. 2015, doi: 10.1109/TDSC.2014.2313861.
- [12] T. Ashur, O. Dunkelman, and A. Luykx, "Boosting authenticated encryption robustness with minimal modifications," in *Advances in Cryptology – CRYPTO 2017*, vol. 10403, 2017, pp. 3–33, doi: 10.1007/978-3-319-63697-9_1.
- [13] A. Luykx, "The design and analysis of message authentication and authenticated encryption schemes," Katholieke University Leuven, 2016.
- [14] W. Yu *et al.*, "A survey on the edge computing for the internet of things," *IEEE Access*, vol. 6, pp. 6900–6919, 2018, doi: 10.1109/ACCESS.2017.2778504.
- [15] A. Yassine, S. Singh, M. S. Hossain, and G. Muhammad, "IoT big data analytics for smart homes with fog and cloud computing," *Future Generation Computer Systems*, vol. 91, pp. 563–573, Feb. 2019, doi: 10.1016/j.future.2018.08.040.
- [16] C.-H. Hong and B. Varghese, "Resource management in fog/edge computing: a survey on architectures, infrastructure, and algorithms," *ACM Computing Surveys*, vol. 52, no. 5, pp. 1–37, Sep. 2020, doi: 10.1145/3326066.
- [17] A. A.-N. Patwary *et al.*, "Towards secure fog computing: a survey on trust management, privacy, authentication, threats and access control," *Electronics*, vol. 10, no. 10, p. 1171, May 2021, doi: 10.3390/electronics10101171.
- [18] M. Mukherjee *et al.*, "Security and privacy in fog computing: challenges," *IEEE Access*, vol. 5, pp. 19293–19304, 2017, doi: 10.1109/ACCESS.2017.2749422.
- [19] Diallo Alhassane, "Enhancement of bluetooth security authentication using hash-based message authentication code (HMAC) algorithm," *PhD diss., Kulliyah of Engineering, International Islamic University Malaysia*, 2015, doi: 10.13140/RG.2.1.1196.0082.
- [20] P. H. Kumar and G. S. AnandhaMala, "HMAC-R: Hash-based message authentication code and Rijndael-based multilevel security model for data storage in cloud environment," *Journal of Supercomputing*, vol. 79, no. 3, pp. 3181–3209, Feb. 2023, doi: 10.1007/s11227-022-04714-x.
- [21] M. Bellare, R. Canetti, and H. Krawczyk, "Keying hash functions for message authentication," in *Advances in Cryptology – CRYPTO '96*, vol. 1109, N. Koblitz, Ed., in Lecture Notes in Computer Science, vol. 1109, Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 1–15, doi: 10.1007/3-540-68697-5_1.
- [22] E. Baccarelli, M. Scarpiniti, P. G. V. Naranjo, and L. Vaca-Cardenas, "Fog of social IoT: When the fog becomes social," *IEEE Network*, vol. 32, no. 4, pp. 68–80, Jul. 2018, doi: 10.1109/MNET.2018.1700031.
- [23] Y. Abuseta, "A fog computing based architecture for iot services and applications development," *International Journal of Computer Trends and Technology*, vol. 67, no. 10, pp. 92–98, Oct. 2019, doi: 10.14445/22312803/IJCTT-V67I10P116.
- [24] C. H. Gebotys, "Data integrity and message authentication," in *Security in Embedded Devices*, Boston, MA: Springer US, 2010, pp. 143–161, doi: 10.1007/978-1-4419-1530-6-7.
- [25] J. Schmandt, A. T. Sherman, and N. Banerjee, "Mini-MAC: Raising the bar for vehicular security with a lightweight message authentication protocol," *Vehicular Communications*, vol. 9, pp. 188–196, Jul. 2017, doi: 10.1016/j.vehcom.2017.07.002.
- [26] N. Kheshaifaty and A. Gutub, "Preventing multiple accessing attacks via efficient integration of captcha crypto hash functions," *International Journal of Computer Science and Network Security*, vol. 20, no. 9, pp. 16–28, Sep. 2020, doi: 10.22937/IJCSNS.2020.20.09.3.
- [27] H. N. Noura, R. Melki, A. Chehab, and J. H. Fernandez, "Efficient and secure message authentication algorithm at the physical layer," *Wireless Network*, Jun. 2020, doi: 10.1007/s11276-020-02371-7.




BIOGRAPHIES OF AUTHORS

Abdelhak Sakhi    completed his higher education in Casablanca, Morocco. He started his PhD in Artificial Intelligence in 2020. Currently, he is a professor of mathematics at the Ministry of Education in Morocco. He can be contacted at email: sakhi442@gmail.com.



Salah-Eddine Mansour    completed his higher education in Casablanca, Morocco. He started his PhD in Artificial Intelligence in 2020. Currently, he is a professor of Informatics at the Ministry of Education in Morocco. He can be contacted at email: 19mansour94@gmail.com.



Abderrahim Sekkaki    completed his graduate studies in Toulouse, France. After having passed his master's degree and his DEA in computer science, he began his PhD in network management, defended in 1991. He crowned his career in computer science with a state thesis in 2002. Currently, he is a full professor in University Hassan II of Casablanca. He can be contacted at email: sekkabd@gmail.com.