Enhancing Security Mechanisms for IoT-Fog Networks

Salah-Eddine Mansour [1*], Abdlehak Sakhi [2], Larbi Kzaz [3], Abderrahim Sekkaki [4]
[1, 2, 4] Electrical and Industrial Engineering Information Processing IT and logistics (GEIIL), Faculty of Sciences Ain Chock, Hassan II University, Casablanca, Morocco
[3] Higher Institute of Commerce and Business Administration (ISCAE), Hassan II University, Casablanca, Morocco
Email: [1]19mansour94@gmail.com, [2] sakhi442@gmail.com, [3] kzaz.larbi@gmail.com, [4] sekkabd@gmail.com

***Abstract*—This study contributes to improving Morocco's fish canning industry by integrating artificial intelligence (AI). The primary objective involves developing an AI and image processing-based system to monitor and guarantee canning process quality in the facility. It commenced with an IoT-enabled device capable of capturing and processing images, leading to the creation of an AI-driven system adept at accurately categorizing improperly crimped cans. Further advancements focused on reinforcing communication between IoT devices and servers housing individual client's neural network weights. These weights are vital, ensuring the functionality of our IoT device. The efficiency of the IoT device in categorizing cans relies on updated neural network weights from the Fog server, crucial for continual refinement and adaptation to diverse can shapes. Securing communication integrity between devices and the server is imperative to avoid disruptions in can classification, emphasizing the need for secure channels. In this paper, our key scientific contribution revolves around devising a security protocol founded on HMAC. This protocol guarantees authentication and preserves the integrity of neural network weights exchanged between Fog computing nodes and IoT devices. The innovative addition of a comprehensive dictionary within the Fog server significantly bolsters security measures, enhancing the overall safety between these interconnected entities.**

Keywords—Cloud Computing; Fog Computing; IoT; HMAC; Hashing.

I. Introduction

This project is part of an industrial initiative aimed at upgrading the fish canning industry in Morocco through the integration of artificial intelligence (AI). Our primary purpose entails creating an AI and image processing-based system to oversee and ensure the quality requirements of the canning process within the facility. Our quest began with creating an IoT-enabled electronic device capable of recording and processing images. Subsequently, we developed an AI-powered system to accurately categorize improperly crimped cans. Progressing further, we reinforced the communication link between these IoT devices and the servers storing each client's neural network weights. These weights are essential; they ensure the proper functionality of our IoT device [1], [2].

The efficiency of the IoT device in precisely categorizing cans relies heavily on the neural network weights it acquires from the Fog server. These weight updates are fundamental components of our ongoing efforts to consistently fine-tune the neural network's performance. Our objective is to elevate the accuracy of classification processes while actively identifying and adapting to emerging can shapes, encompassing diverse forms such as cubic or cylindrical variations.

The significance of these weight updates lies in their role as catalysts for refinement, enabling our neural network to evolve continuously. By refining the network's parameters, we strive not only to enhance accuracy but also to ensure adaptability to newer can shapes that might enter the market.

Securing the communication link between our device and the server stands as a critical measure to uphold the integrity of these weight values. The unaltered transmission of these weights is imperative. Any tampering or modifications during transmission could severely disrupt the device's inherent capability to accurately classify cans, particularly those with deformities. Such disruptions pose a tangible risk of incurring production losses, emphasizing the indispensable need for secure and reliable communication channels to preserve the integrity of our neural network weights.

Certainly! Our contribution involves crafting a security protocol reliant on HMAC, enabling both the Fog computing node and IoT devices to authenticate themselves and ensure message integrity during their communications [3]–[5]. 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.

In this study, Section 2 will go into the existing literature, investigating relevant studies in the topic. Section 3 will emphasize our specific contribution, concentrating on strengthening security for Fog-IoT communication through the implementation of the HMAC Protocol. Subsequently, Section 4 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.

II. Related Works

Authentication methods encompass various structures, one of which is the Cipher-based Message Authentication Code (CMAC). This technique relies on a strong cryptographic foundation, typically leveraging a block cipher like AES (Advanced Encryption Standard) operating in Cipher Block Chaining (CBC) mode [6], [7]. By utilizing a private secret key shared between the sender and recipient, CMAC processes fixed-size data blocks, potentially applying padding if the message size isn't a multiple of the block size. It employs the block cipher in CBC mode with a tweak, altering the final block cipher operation to generate an authentication tag or MAC. CMAC boasts robust security measures, resilience against specific attacks, and efficiency in constructing fixed-size authentication tags. It's often employed in protocols and applications where ensuring message integrity and authenticity holds utmost importance [8]–[10].

Similarly, Galois/Counter Mode (GCM) describes a symmetric critical cryptographic mode used with the Advanced Encryption Standard (AES) to achieve authenticated encryption [11]. This approach combines encryption and authentication, ensuring data secrecy and integrity verification. GCM leverages AES encryption's counter mode (CTR), generating a keystream by encrypting successive counter values. Notably, it leverages Galois field multiplication to construct an authentication tag, enabling verification of both data authenticity and integrity. Renowned for its efficiency, particularly in hardware implementations, GCM finds extensive application in safeguarding network communications, including Wi-Fi protocols (such as WPA2 WPA3), Transport Layer Security (TLS), IPsec, and several other security protocols. With a strong cipher like AES, GCM offers solid security, balancing high-grade protection and computational performance [12], [13].

In addition, KMAC stands as a versatile cryptographic structure anchored in the KECCAK function, a core component of the SHA-3 family. Leveraging the configurable nature of its design, KMAC enables the inclusion of a customization string, providing users the flexibility to modify its functioning to specific security settings or requirements its versatility stretches across cryptographic demands, enabling message authentication, hashing, and key derivation. From the solid security qualities inherent in the SHA-3 family, KMAC retains a strong cryptographic foundation, playing a crucial role in post-quantum cryptography and cryptographic standardization efforts by groups like the National Institute of Standards and Technology (NIST) [14]–[16].

Finally, there is Poly1305, a cryptographic message authentication code (MAC) function paired with a secret key that offers message integrity and authenticity [17], [18]. It is frequently used with symmetric encryption algorithms like AES-GCM (Advanced Encryption Standard-Galois/Counter Mode) to create authenticated encryption. By evaluating a polynomial function over a finite field, Poly1305 delivers a fixed-size authentication tag for a message and key pair. It delivers solid security when built correctly, resists timing attacks, and boasts efficient performance. It is intended for applications demanding comprehensive data integrity checks and authentication while maintaining computational performance [19].

III. Method

A. IoT Device

The IoT device comprises three key electronic components, as illustrated in figure 1. Firstly, it integrates a GOPRO HERO9 camera capable of capturing 60 frames per second (60fps), ensuring high-quality image capture regardless of the production series' speed [20], [21]. Notably, the camera's open-gopro library, accessible in Python, allows for effective control (see Fig. 1, component A).

The second essential component is the Raspberry Pi 4 processing unit, equipped with 8 GB of RAM, a robust microprocessor, and an open-source Debian-based operating system. This unit houses our classification program and an Application Programming Interface (API) for seamless communication with the Fog computing node [22]–[24]. Our significant scientific contribution lies in the meticulous security measures implemented to safeguard the received neural network weights from the Fog computing node (see Fig. 1, component B).

Finally, the IoT device integrates an HC-SR04 ultrasonic sensor, adept at detecting the presence of cans within a suitable position with an effective measurement angle of 15°. Each component plays a pivotal role in the device's comprehensive functionality, from high-speed image capture to neural network updates and precise can detection (see Fig. 1, component C) [25].

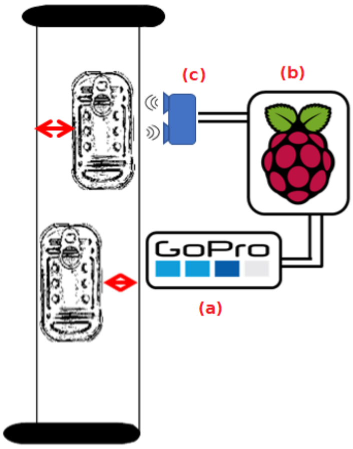

Fig. 1. The foundational elements comprising an IoT device integrated within the production line.

B. Fog Computing Architecture

The fog computing architecture, illustrated in Fig. 2, employs a tiered structure designed to optimize data processing, storage, and computation near the network edge. Its aim is to improve efficiency and reduce latency. At the foundation are multiple Edge Devices that consist of sensors, actuators, and IoT devices. They play a crucial role in generating and gathering data at the network's periphery, serving as the primary points for information entry into the fog computing ecosystem [26]–[28].

The intermediate tier consists of Fog Nodes strategically located nearer to the edge devices, unlike traditional centralized cloud data centers. These nodes function as pivotal processing hubs, executing applications, offering storage, and delivering vital network services. They encompass various devices like routers, switches, and specialized hardware, all finely tuned to efficiently manage tasks within the fog computing paradigm [29], [30].

The computational potential of fog nodes is harnessed by Fog Services and Applications. These services manage data processing, analytics, and instantaneous decision-making tailored to specific use cases and operational needs

The Fog Orchestration and Management Layer effectively coordinates and supervises resource distribution within the fog computing infrastructure. This layer oversees crucial tasks such as resource allocation, security enforcement, and continuous monitoring of fog nodes and services [31]–[33].

Enabling uninterrupted links between edge devices and fog nodes, the Connectivity and Networking Layer ensures efficient data transmission and communication. It utilizes various technologies such as edge routers, wireless networks, and protocols to facilitate seamless interactions.

Integral to the comprehensive design, the Security and Privacy Layer integrates robust methods like encryption, authentication, access control, and secure communication protocols. These techniques serve to protect data and communications, guaranteeing the integrity and security of information within the fog computing environment. The decentralized nature of fog computing optimizes data processing by placing computational resources nearer to the source. This enables quicker processing, minimized latency, and enhanced efficiency for real-time applications across various industries and domains [34].

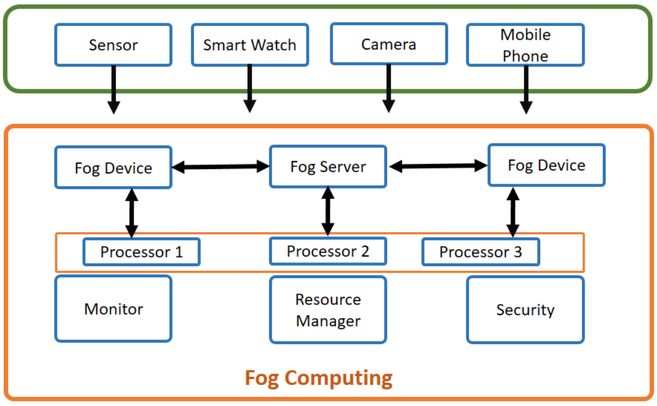

Fig. 2. Fog computing architecture

C. Hash-based Message Authentication Code

Hash-based Message Authentication Code (HMAC) represents a commonly used cryptographic construct meant to validate the integrity and origin of messages, ensuring secure communication over potentially insecure channels [35], [36]. 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 [37]–[39]. 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.

One of HMAC's primary advantages is its versatility and application across multiple security protocols and systems. It's extensively applied in internet security protocols like TLS (Transport Layer Security) and IPsec (Internet Protocol Security), 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 [40], [41].

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. As processing power develops, earlier hash functions can become vulnerable to attacks, thus undermining the security of HMAC [42]. 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 [43]–[45].

Within our canning industry operations, a pressing concern revolves around enabling our IoT device to securely and equitably receive crucial neural network weights from the server [46]. This challenge stems from the necessity to ensure that the transmission of these capabilities from the Fog computing node to our device occurs in a manner that's both secure and unbiased. Addressing this challenge is imperative for the uninterrupted and effective functioning of our device in classifying cans accurately and efficiently.

To resolve this, a meticulously designed protocol has been introduced as a solution. HMAC operates as a comprehensive framework aimed at facilitating the secure and fair transmission of neural network capabilities. Central to its functionality is the implementation of MAC (Message Authentication Code) verification within the IoT device [47]–[49]. Through this verification process, the integrity of the weights and configurations received from the Fog computing node is rigorously checked. This meticulous scrutiny ensures that any alterations or unauthorized modifications during transmission are promptly identified, preserving the sanctity and authenticity of the neural network capabilities obtained by our device. By employing this protocol, we establish a robust system that not only upholds security but also guarantees fairness in the acquisition of vital neural network capabilities, fostering reliable and accurate can classification within our industry processes [50]–[52].

D. IoT-Fog Security

Within the IoT-Fog framework, ensuring mutual authentication among interconnected devices emerges as a critical security priority. As IoT devices commonly operate under limited battery capacities and frequent data transmission needs, integrating a lightweight authentication mechanism becomes pivotal in minimizing energy consumption. Our proposed solution addresses this authentication requirement between a Fog computing node and multiple IoT devices [53]. The strategy involves leveraging the HMAC protocol alongside a compact database functioning as a repository for the unique IDs and corresponding secret keys of each IoT device. This approach effectively segregates the transmitted data at both the hashing and security layers between the node and the devices. Fig. 3 provides a schematic depiction of our network infrastructure, showcasing the integration between IoT devices and the Fog server. In the subsequent section, we'll delve into the specific security protocol implemented for communication between the node and the IoT devices [54], [55].

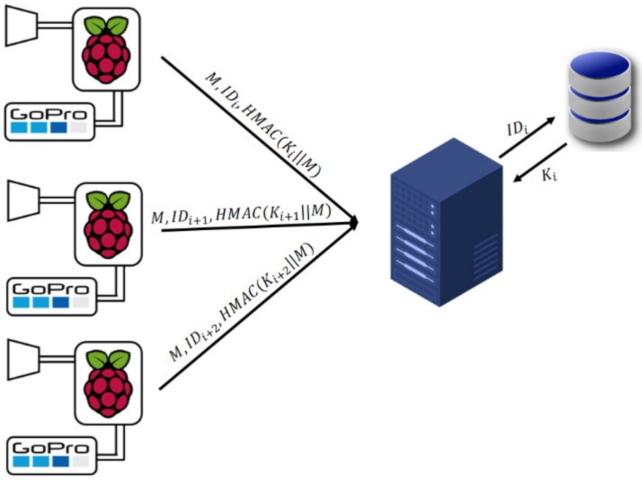
$M, ID_i, HMAC(K_i||M)$
$M, ID_{i+1}, HMAC(K_{i+1}||M)$
$M, ID_{i+2}, HMAC(K_{i+2}||M)$
ID_i
K_i
GoPro
GoPro
GoPro

Fig. 3. Integrated network infrastructure: uniting iot devices, the fog server, and database

Before the IoT device gains access to the essential neural network weight values, it engages in an intricate initiation sequence, as we see in Fig. 4. This sequence begins with the device transmitting its unique Identifier (ID) to the Fog server, a crucial step initiating the authentication process. The server, acting as the gatekeeper, meticulously verifies the presence and validity of this ID within its database. This serves as the initial checkpoint ensuring the device's legitimacy within the network.

Upon successful verification of the ID, the Fog server responds by dispatching a random value (N) to the awaiting IoT device. This random value, a cryptographic challenge, prompts the IoT device to showcase its authenticity by employing HMAC encryption. The device utilizes this random value along with a secret key (K), shared exclusively between the IoT device and the server. This process, executed through HMAC hashing, serves as a robust means of validation, affirming the device's rightful place and authorization within the network.

Successfully navigating this authentication challenge enables the IoT device to establish its trustworthiness and validated association within the network infrastructure. Upon this verification, the server securely shares the requested neural network weight values with the IoT device. To ensure the integrity of this data transmission, the server accompanies the weight values with a corresponding MAC value, generated using HMAC. This meticulous security protocol not only validates the device's legitimacy but also guarantees the unaltered and secure transfer of critical neural network weight values between the IoT device and the server.

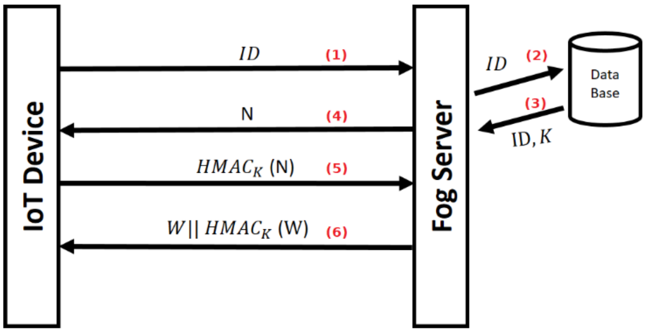

Fig. 4. Protocol sequencing: iot device, fog computing node, and database communication steps

Now that we've familiarized ourselves with our network infrastructure and its inter-element communication protocol, let's delve into an in-depth exploration of HMAC, along with the latest advancements incorporated into this cryptographic method. As we see in Fig. 5, 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. 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.

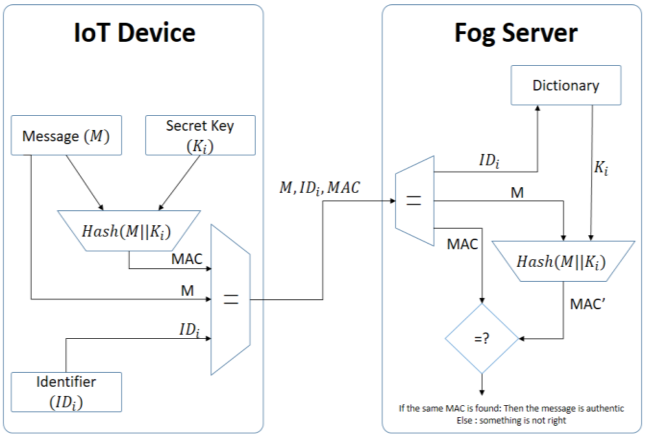

Fig. 5. Verification mechanism ensuring message integrity

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 Idi, are received and processed.

The process continues by relaying the identifier Idi to the database to retrieve the corresponding secret key Ki associated with the specific IoT device. With the secret key Ki in hand, the same hash function used earlier (e.g., SHA256, MD5) is executed using the retrieved key and the received message. This step generates a recalculated MAC', serving as a new verification code [56].

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 [57]. 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.

IV. 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 [58], [59]. By employing the Hashed Message Authentication Code (HMAC) function, the protocol generates a hash using a shared secret. 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 [61].

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 [62]–[64].

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 [65], [66]. This stringent access control paradigm ensures that only authorized devices with registered IDs can leverage and benefit from the services provided by the system.

Looking from a different perspective, a range of hashing methods, including HMAC, is available for facilitating communication between the IoT Device and the Fog computing node. However, our selection of HMAC wasn't random; it was the outcome of a thorough energy-focused comparison among hashing methods—CMAC, KMAC, GCM, and Poly1305—outlined earlier in this article. This decision was the result of a careful evaluation centered on the energy efficiency of these various methods [67]–[69]. HMAC implementations generally maintain computational efficiency with moderate energy demands, utilizing hash function operations like SHA-256 alongside key manipulation. CMAC, involving block cipher operations such as AES, tends to consume more energy due to multiple encryption rounds, offering robust security but potentially impacting performance. KMAC, based on the KECCAK sponge construction, demonstrates moderate energy requirements aligned with the SHA-3 standard but might marginally exceed energy usage compared to simpler hash-based schemes [70], [71]. GCM, combining symmetric encryption like AES with Galois field multiplication, potentially consumes moderate energy, providing both confidentiality and authentication efficiency but susceptible to certain side-channel attacks. In contrast, Poly1305, primarily using polynomial multiplication operations, excels in energy efficiency, providing authentication but requiring an additional encryption mechanism for confidentiality. While Poly1305 and HMAC tend to exhibit better energy efficiency compared to algorithms like CMAC, KMAC, or GCM, the specifics of hardware, implementation, and workloads significantly influence energy consumption, urging a balanced assessment considering security, efficiency, and application requisites [72]–[74].

In this assessment of energy-level protocols, we examine and contrast the fundamental hashing and encryption algorithms—SHA-256, SHA-3, and AES—integral to these protocols [75]–[77]. To aid our decision-making regarding the implementation of HMAC, we offer estimated processing times for encryption operations using these algorithms as standard benchmarks. This comparative analysis is crucial for understanding their unique efficiencies and acts as a guiding tool to evaluate whether HMAC is well-suited for our specific use case [78].

The timings presented below were obtained using the Raspberry Pi Zero W, a device with limited resources. This device performed speed tests on different cryptographic hash functions used in HMAC, Poly1305, and CMAC [79]–[81]. The table demonstrates variations in timing among these hash functions when generating digests on a 32-bit CPU (Table I).

TABLE I. Average Timings Related to Different Hash Functions

Message Length (Bytes)	8	16	32	64	128
SHA-256	0.002372	0.002451	0.002493	0.002532	0.002583
SHA3-256	0.004359	0.004455	0.004393	0.004464	0.004383
AES	0.00869	0.008855	0.009682	0.010406	0.012079

It's notable that AES is the slower algorithm than the SHA family. Additionally, in this test, we observed that SHA3-256 operates marginally slower in processing speed compared to SHA-256. The distinctive design of SHA3, rooted in the Keccak algorithm, involves different operations and structure compared to SHA-256, which can influence its overall speed.

V. Conclusion

In this paper, we've underscored the pivotal importance of updated neural network weights exchanged via Fog servers to ensure precise can categorization, advocating the use of a secure HMAC-based protocol to safeguard this communication. Furthermore, the integration of a comprehensive dictionary within the Fog server has significantly fortified security, effectively segregating communication channels between the server and individual IoT devices. In essence, our research centered on ensuring fair and secure transmission of neural network weights from servers to devices. However, our future research aims to introduce additional solutions aimed at encrypting these weights. This endeavor intends to prevent any unauthorized exploitation without proper permission by ensuring that eavesdropping on these critical resources is impossible

Acknowledgment

We extend our heartfelt appreciation to the National Center for Scientific and Technical Research (CNRST) in Morocco for their invaluable support and guidance during the entire span of this research endeavor. Their unwavering dedication to advancing scientific exploration and their integral role in steering our research pursuits have been pivotal to the accomplishment of this project, aligned with the Al-Khwarizmi Program.

References

[1] S. Thouti, N. Venu, D. R. Rinku, A. Arora, and N. Rajeswaran, "Investigation on identify the multiple issues in IoT devices using Convolutional Neural Network," *Meas. Sens.*, vol. 24, p. 100509, Dec. 2022, doi: 10.1016/j.measen.2022.100509.

[2] M. Ficco, A. Guerriero, E. Milite, F. Palmieri, R. Pietrantuono, and S. Russo, "Federated learning for IoT devices: Enhancing TinyML with on-board training," *Inf. Fusion*, vol. 104, p. 102189, Apr. 2024, doi: 10.1016/j.inffus.2023.102189.

[3] P. Reedy, "Interpol review of digital evidence for 2019–2022," *Forensic Sci. Int. Synergy*, vol. 6, p. 100313, 2023, doi: 10.1016/j.fsisyn.2022.100313.

[4] M. Asghar, L. Pan, and R. Doss, "An efficient voting based decentralized revocation protocol for vehicular ad hoc networks," *Digit. Commun. Netw.*, vol. 6, no. 4, pp. 422–432, Nov. 2020, doi: 10.1016/j.dcan.2020.03.001.

[5] S. K. Khare, "Fast-track message authentication protocol for DSRC using HMAC and group keys," *Appl. Acoust.*, vol. 165, p. 107331, Aug. 2020, doi: 10.1016/j.apacoust.2020.107331.

[6] P. Prajapati and K. Chaudhari, "KBC: Multiple Key Generation using Key Block Chaining," *Procedia Comput. Sci.*, vol. 167, pp. 1960–1969, 2020, doi: 10.1016/j.procs.2020.03.224.

[7] M. E. Hameed, M. M. Ibrahim, N. A. Manap, and A. A. Mohammed, "A lossless compression and encryption mechanism for remote monitoring of ECG data using Huffman coding and CBC-AES," *Future Gener. Comput. Syst.*, vol. 111, pp. 829–840, Oct. 2020, doi: 10.1016/j.future.2019.10.010.

[8] S. Jarillo and J. Barnett, "Contingent communality and community-based adaptation to climate change: Insights from a Pacific rural atoll," *J. Rural Stud.*, vol. 87, pp. 137–145, Oct. 2021, doi: 10.1016/j.jrurstud.2021.08.026.

[9] M. Vít et al., "A broad tuneable birdcage coil for mouse 1H/19F MR applications," *J. Magn. Reson.*, vol. 329, p. 107023, Aug. 2021, doi: 10.1016/j.jmr.2021.107023.

[10] L. L. De Taeye, M. J. Mees, and P. M. Vereecken, "Surpassing the 1 Li/Ti capacity limit in chlorine modified TiO 2 − y Cl 2 y," *Energy Storage Mater.*, vol. 36, pp. 279–290, Apr. 2021, doi: 10.1016/j.ensm.2020.12.030.

[11] S. A. Abdel Hakeem and H. Kim, "Authentication and encryption protocol with revocation and reputation management for enhancing 5G-V2X security," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 7, p. 101638, Jul. 2023, doi: 10.1016/j.jksuci.2023.101638.

[12] H. Bühler, A. Walz, and A. Sikora, "Benchmarking of Symmetric Cryptographic Algorithms on a Deeply Embedded System," *IFAC-Pap.*, vol. 55, no. 4, pp. 266–271, 2022, doi: 10.1016/j.ifacol.2022.06.044.

[13] B. Mohinder Singh and J. Natarajan, "A novel secure authentication protocol for eHealth records in cloud with a new key generation method and minimized key exchange," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 7, p. 101629, Jul. 2023, doi: 10.1016/j.jksuci.2023.101629.

[14] Y. Baek and S. Shin, "CANon: Lightweight and Practical Cyber-Attack Detection for Automotive Controller Area Networks," *Sensors*, vol. 22, no. 7, p. 2636, Mar. 2022, doi: 10.3390/s22072636.

[15] Q. Fei, "Traditional Chinese Medicine Treatment, Gua Sha, can Induce Subtle Molecular Changes in Gene Expression," Biomed Env. Sci.

[16] L. T. Piame, P. M. Kaktcham, E. M. F. Kouam, U. D. F. Techeu, R. J. Ngouénam, and F. Z. Ngoufack, "Technological characterisation and probiotic traits of yeasts isolated from Sha'a, a Cameroonian maize-based traditional fermented beverage," *Heliyon*, vol. 8, no. 10, p. e10850, Oct. 2022, doi: 10.1016/j.heliyon.2022.e10850.

[17] R. D. Sole, T. Stomeo, and L. Mergola, "Disposable Molecularly Imprinted Polymer-Modified Screen-Printed Electrodes for Rapid Electrochemical Detection of l-Kynurenine in Human Urine," *Polymers*, vol. 16, no. 1, p. 3, Dec. 2023, doi: 10.3390/polym16010003.

[18] S. Sentanoe and H. P. Reiser, "SSHkex: Leveraging virtual machine introspection for extracting SSH keys and decrypting SSH network traffic," *Forensic Sci. Int. Digit. Investig.*, vol. 40, p. 301337, Apr. 2022, doi: 10.1016/j.fsidi.2022.301337.

[19] F. Breitinger, X. Zhang, and D. Quick, "A forensic analysis of rclone and rclone's prospects for digital forensic investigations of cloud storage," *Forensic Sci. Int. Digit. Investig.*, vol. 43, p. 301443, Sep. 2022, doi: 10.1016/j.fsidi.2022.301443.

[20] R. Matos *et al.*, "Tactical Knowledge by Decision Making and Motor Efficiency of Young Football Players in Different Playing Positions during a Three-a-Side Small-Sided Game," *Behav. Sci.*, vol. 13, no. 4, p. 310, Apr. 2023, doi: 10.3390/bs13040310.

[21] Z. Ma, X. Zhong, H. Xie, Y. Zhou, Y. Chen, and J. Wang, "A Combined Physical and Mathematical Calibration Method for Low-Cost Cameras in the Air and Underwater Environment," *Sensors*, vol. 23, no. 4, p. 2041, Feb. 2023, doi: 10.3390/s23042041.

[22] D. P. Hausherr and D. Berben, "(All-in-One) Power Supply System for Mobile and Network-Wired Raspberry Pi-Based Internet of Things Applications," *Hardware*, vol. 1, no. 1, pp. 54–69, Dec. 2023, doi: 10.3390/hardware1010005.

[23] A. Khan, K. S. Khattak, Z. H. Khan, T. A. Gulliver, and Abdullah, "Edge Computing for Effective and Efficient Traffic Characterization," *Sensors*, vol. 23, no. 23, p. 9385, Nov. 2023, doi: 10.3390/s23239385.

[24] S. B. Rosende, S. Ghisler, J. Fernández-Andrés, and J. Sánchez-Soriano, "Implementation of an Edge-Computing Vision System on Reduced-Board Computers Embedded in UAVs for Intelligent Traffic Management," *Drones*, vol. 7, no. 11, p. 682, Nov. 2023, doi: 10.3390/drones7110682.

[25] P. Akhil, R. Akshara, R. Athira, S. P. Kamalesh Kumar, M. Thamotharan, and S. Shobha Christila, "Smart Blind Walking Stick with Integrated Sensor," in *The 2nd International Conference on Innovative Research in Renewable Energy Technologies (IRRET 2022)*, p. 12, Sep. 2022, doi: 10.3390/materproc2022010012.

[26] H. Chen, X. Chen, L. Peng, and Y. Bai, "Personalized Fair Split Learning for Resource-Constrained Internet of Things," *Sensors*, vol. 24, no. 1, p. 88, 2023.

[27] T. Vandervelden, D. Deac, R. Van Glabbeek, R. De Smet, A. Braeken, and K. Steenhaut, "Evaluation of 6LoWPAN Generic Header Compression in the Context of a RPL Network," *Sensors*, vol. 24, no. 1, p. 73, Dec. 2023, doi: 10.3390/s24010073.

[28] A. S. Al-Khaleefa, G. F. K. Al-Musawi, and T. J. Saeed, "IoT-Based Framework for COVID-19 Detection Using Machine Learning Techniques," *Sci*, vol. 6, no. 1, p. 2, 2023.

[29] M. Biabani, N. Yazdani, and H. Fotouhi, "Developing a Novel Hierarchical VPLS Architecture Using Q-in-Q Tunneling in Router and Switch Design," *Computers*, vol. 12, no. 9, p. 180, Sep. 2023, doi: 10.3390/computers12090180.

[30] A. Munshi, "Hybrid Detection Technique for IP Packet Header Modifications Associated with Store-and-Forward Operations," *Appl. Sci.*, vol. 13, no. 18, p. 10229, Sep. 2023, doi: 10.3390/app131810229.

[31] T. Xiao, T. Cui, S. M. R. Islam, and Q. Chen, “Joint Content Placement and Storage Allocation Based on Federated Learning in F-RANs,” *Sensors*, vol. 21, no. 1, p. 215, Dec. 2020, doi: 10.3390/s21010215.

[32] A. Bani-Bakr *et al.*, “Optimizing the Number of Fog Nodes for Finite Fog Radio Access Networks under Multi-Slope Path Loss Model,” *Electronics*, vol. 9, no. 12, p. 2175, Dec. 2020, doi: 10.3390/electronics9122175.

[33] A. Aldalbahi, M. A. Jasim, N. Siasi, M. Bouzguenda, H. Enshasy, and R. Sumsudeen, “Clustered and Distributed Caching Methods for F-RAN-Based mmWave Communications,” *Appl. Sci.*, vol. 12, no. 14, p. 7111, Jul. 2022, doi: 10.3390/app12147111.

[34] I. Ungurean and N. C. Gaitan, “A Dynamic IIoT Framework Based on the Publish–Subscribe Paradigm,” *Sensors*, vol. 23, no. 24, p. 9829, Dec. 2023, doi: 10.3390/s23249829.

[35] Ö. Şeker, G. Dalkılıç, and U. C. Çabuk, “MARAS: Mutual Authentication and Role-Based Authorization Scheme for Lightweight Internet of Things Applications,” *Sensors*, vol. 23, no. 12, p. 5674, Jun. 2023, doi: 10.3390/s23125674.

[36] F. Páez and H. Kaschel, “Design and Testing of a Computer Security Layer for the LIN Bus,” *Sensors*, vol. 22, no. 18, p. 6901, Sep. 2022, doi: 10.3390/s22186901.

[37] A. Alotaibi, A. Ibrahim, R. Ahmed, and T. Abualait, “Effectiveness of Partial Body Weight-Supported Treadmill Training on Various Outcomes in Different Contexts among Children and Adolescents with Cerebral Palsy: A Systematic Review and Meta-Analysis,” *Children*, vol. 11, no. 1, p. 9, Dec. 2023, doi: 10.3390/children11010009.

[38] K. Joseph, O. S. Eyobu, P. Kasyoka, and T. J. Oyana, “A Link Fabrication Attack Mitigation Approach (LiFAMA) for Software Defined Networks,” *Electronics*, vol. 11, no. 10, p. 1581, May 2022, doi: 10.3390/electronics11101581.

[39] W. Fan, Q. Liu, X. Zhang, Y. Gao, X. Qi, and X. Wang, “A Symmetric and Multilayer Reconfigurable Architecture for Hash Algorithm,” *Electronics*, vol. 12, no. 13, p. 2872, Jun. 2023, doi: 10.3390/electronics12132872.

[40] A. F. Gentile, D. Macrì, F. De Rango, M. Tropea, and E. Greco, “A VPN Performances Analysis of Constrained Hardware Open Source Infrastructure Deploy in IoT Environment,” *Future Internet*, vol. 14, no. 9, p. 264, Sep. 2022, doi: 10.3390/fi14090264.

[41] Z. Sui, H. Shu, F. Kang, Y. Huang, and G. Huo, “A Comprehensive Review of Tunnel Detection on Multilayer Protocols: From Traditional to Machine Learning Approaches,” *Appl. Sci.*, vol. 13, no. 3, p. 1974, Feb. 2023, doi: 10.3390/app13031974.

[42] Q. Xia *et al.*, “Using Phenol Formaldehyde Resin, Hexamethylenetetramine and Matrix Asphalt to Synthesize Hard-Grade Asphalts for High-Modulus Asphalt Concrete,” *Sustainability*, vol. 14, no. 23, p. 15689, Nov. 2022, doi: 10.3390/su142315689.

[43] A. Venčkauskas, N. Morkevicius, K. Bagdonas, R. Damaševičius, and R. Maskeliūnas, “A Lightweight Protocol for Secure Video Streaming,” *Sensors*, vol. 18, no. 5, p. 1554, May 2018, doi: 10.3390/s18051554.

[44] M. Iwański *et al.*, “Stiffness Evaluation of Laboratory and Plant Produced Foamed Bitumen Warm Asphalt Mixtures with Fiber Reinforcement and Bio-Flux Additive,” *Materials*, vol. 16, no. 5, p. 1950, Feb. 2023, doi: 10.3390/ma16051950.

[45] N. A. Mohd Khatib, A. Roseliza-Murni, S. Mohd Hoesni, and J. Manap, “Adolescent Connectedness: Testing Confirmatory Factor Analysis of the Hemingway: Measure of Adolescent Connectedness–Bahasa Melayu Version (HMAC–BM),” *Int. J. Environ. Res. Public. Health*, vol. 19, no. 19, p. 12189, Sep. 2022, doi: 10.3390/ijerph191912189.

[46] K. Chakraborty, D. Kapila, S. Kumar, Bhupati, N. Shaik, and A. Singh, “Intelligent Machine Learning Based Internet of Things (IoT) Resource Allocation,” in *RAiSE-2023*, p. 73, Dec. 2023, doi: 10.3390/engproc2023059073.

[47] E. V. D. Subramaniam, K. Srinivasan, S. M. Qaisar, and P. Pławiak, “Interoperable IoMT Approach for Remote Diagnosis with Privacy-Preservation Perspective in Edge Systems,” *Sensors*, vol. 23, no. 17, p. 7474, Aug. 2023, doi: 10.3390/s23177474.

[48] A. A. Khamis *et al.*, “Development and Performance Evaluation of an IoT-Integrated Breath Analyzer,” *Int. J. Environ. Res. Public. Health*, vol. 20, no. 2, p. 1319, Jan. 2023, doi: 10.3390/ijerph20021319.

[49] J. L. Gonzalez-Compean, V. J. Sosa-Sosa, J. J. Garcia-Hernandez, H. Galeana-Zapien, and H. G. Reyes-Anastacio, “A Blockchain and Fingerprinting Traceability Method for Digital Product Lifecycle Management,” *Sensors*, vol. 22, no. 21, p. 8400, Nov. 2022, doi: 10.3390/s22218400.

[50] C. Fu *et al.*, “SqueezeGCN: Adaptive Neighborhood Aggregation with Squeeze Module for Twitter Bot Detection Based on GCN,” *Electronics*, vol. 13, no. 1, p. 56, Dec. 2023, doi: 10.3390/electronics13010056.

[51] Z. Yao *et al.*, “Identification of Milk Adulteration in Camel Milk Using FT-Mid-Infrared Spectroscopy and Machine Learning Models,” *Foods*, vol. 12, no. 24, p. 4517, Dec. 2023, doi: 10.3390/foods12244517.

[52] X. Zheng, R. Feng, J. Fan, W. Han, S. Yu, and J. Chen, “MSISR-STF: Spatiotemporal Fusion via Multilevel Single-Image Super-Resolution,” *Remote Sens.*, vol. 15, no. 24, p. 5675, Dec. 2023, doi: 10.3390/rs15245675.

[53] A. N. Alvi, B. Ali, M. S. Saleh, M. Alkhathami, D. Alsadie, and B. Alghamdi, “TETES: Trust Based Efficient Task Execution Scheme for Fog Enabled Smart Cities,” *Appl. Sci.*, vol. 13, no. 23, p. 12799, Nov. 2023, doi: 10.3390/app132312799.

[54] A. I. A. Alzahrani, A. Al-Rasheed, A. Ksibi, M. Ayadi, M. M. Asiri, and M. Zakariah, “Anomaly Detection in Fog Computing Architectures Using Custom Tab Transformer for Internet of Things,” *Electronics*, vol. 11, no. 23, p. 4017, Dec. 2022, doi: 10.3390/electronics11234017.

[55] M. Balfaqih, W. Jabbar, M. Khayyat, and R. Hassan, “Design and Development of Smart Parking System Based on Fog Computing and Internet of Things,” *Electronics*, vol. 10, no. 24, p. 3184, Dec. 2021, doi: 10.3390/electronics10243184.

[56] Z. Wei, R. He, Y. Li, and C. Song, “DRL-Based Computation Offloading and Resource Allocation in Green MEC-Enabled Maritime-IoT Networks,” *Electronics*, vol. 12, no. 24, p. 4967, Dec. 2023, doi: 10.3390/electronics12244967.

[57] R. Terris-Gallego, I. Fernandez-Hernandez, J. A. López-Salcedo, and G. Seco-Granados, “E1-E6 SDR Platform Based on BladeRF for Testing Galileo-Assisted Commercial Authentication Service,” *Engineering Proceedings*, vol. 54, no. 1, p. 29, 2023.

[58] D. Gupta, S. Wadhwa, S. Rani, Z. Khan, and W. Boulila, “EEDC: An Energy Efficient Data Communication Scheme Based on New Routing Approach in Wireless Sensor Networks for Future IoT Applications,” *Sensors*, vol. 23, no. 21, p. 8839, Oct. 2023, doi: 10.3390/s23218839.

[59] S. Sadhwani, B. Manibalan, R. Muthalagu, and P. Pawar, “A Lightweight Model for DDoS Attack Detection Using Machine Learning Techniques,” *Appl. Sci.*, vol. 13, no. 17, p. 9937, Sep. 2023, doi: 10.3390/app13179937.

[60] H. N. Noura, R. Melki, A. Chehab, and J. Hernandez Fernandez, “Efficient and secure message authentication algorithm at the physical layer,” *Wirel. Netw.*, pp. 1-15, Jun. 2020, doi: 10.1007/s11276-020-02371-7.

[61] D. Dinculeană and X. Cheng, “Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices,” *Appl. Sci.*, vol. 9, no. 5, p. 848, Feb. 2019, doi: 10.3390/app9050848.

[62] M. Bolanowski, A. Paszkiewicz, T. Żabiński, G. Piecuch, M. Salach, and K. Tomecki, “System Architecture for Diagnostics and Supervision of Industrial Equipment and Processes in an IoE Device Environment,” *Electronics*, vol. 12, no. 24, p. 4935, Dec. 2023, doi: 10.3390/electronics12244935.

[63] S. Tjukovs, D. Surmacs, J. Grizans, C. V. Iheanacho, and D. Pikulins, “Implementation of Buck DC-DC Converter as Built-In Chaos Generator for Secure IoT,” *Electronics*, vol. 13, no. 1, p. 20, Dec. 2023, doi: 10.3390/electronics13010020.

[64] T. Cultice, J. Clark, W. Yang, and H. Thapliyal, “A Novel Hierarchical Security Solution for Controller-Area-Network-Based 3D Printing in a Post-Quantum World,” *Sensors*, vol. 23, no. 24, p. 9886, Dec. 2023, doi: 10.3390/s23249886.

[65] S. Ju and Y. Park, “Provably Secure Lightweight Mutual Authentication and Key Agreement Scheme for Cloud-Based IoT Environments,” *Sensors*, vol. 23, no. 24, p. 9766, Dec. 2023, doi: 10.3390/s23249766.

[66] S. Shuai, Z. Hu, B. Zhang, H. B. Liaqat, and X. Kong, “Decentralized Federated Learning-Enabled Relation Aggregation for Anomaly

Detection," *Information*, vol. 14, no. 12, p. 647, Dec. 2023, doi: 10.3390/info14120647.

[67] A. Podevyn, S. Van Vlierberghe, P. Dubruel, and R. Hoogenboom, "Design and Synthesis of Hybrid Thermo-Responsive Hydrogels Based on Poly(2-oxazoline) and Gelatin Derivatives," *Gels*, vol. 8, no. 2, p. 64, Jan. 2022, doi: 10.3390/gels8020064.

[68] G. Serrano *et al.*, "Physiological Performance and Biosorption Capacity of Exiguobacterium sp. SH31 Isolated from Poly-Extreme Salar de Huasco in the Chilean Altiplano: A Study on Rare-Earth Element Tolerance," *Processes*, vol. 12, no. 1, p. 47, 2024.

[69] A. Sideris, T. Sanida, and M. Dasygenis, "A Novel Hardware Architecture for Enhancing the Keccak Hash Function in FPGA Devices," *Information*, vol. 14, no. 9, p. 475, Aug. 2023, doi: 10.3390/info14090475.

[70] A. Dolmeta, M. Martina, and G. Masera, "Comparative Study of Keccak SHA-3 Implementations," *Cryptography*, vol. 7, no. 4, p. 60, Nov. 2023, doi: 10.3390/cryptography7040060.

[71] H. Mestiri and I. Barraj, "High-Speed Hardware Architecture Based on Error Detection for KECCAK," *Micromachines*, vol. 14, no. 6, p. 1129, May 2023, doi: 10.3390/mi14061129.

[72] Y. B. Kim, T.-Y. Youn, and S. C. Seo, "Chaining Optimization Methodology: A New SHA-3 Implementation on Low-End Microcontrollers," *Sustainability*, vol. 13, no. 8, p. 4324, Apr. 2021, doi: 10.3390/su13084324.

[73] A. Braeken, "Highly Efficient Symmetric Key Based Authentication and Key Agreement Protocol Using Keccak," *Sensors*, vol. 20, no. 8, p. 2160, Apr. 2020, doi: 10.3390/s20082160.

[74] N. C. Valencia, M. Izadifar, N. Ukrainczyk, and E. Koenders, "Coarse-Grained Monte Carlo Simulations with Octree Cells for Geopolymer Nucleation at Different pH Values," *Materials*, vol. 17, no. 1, p. 95, 2024.

[75] H. Hashim, A. R. Alzighaibi, A. F. Elessawy, I. Gad, H. Abdul-Kader, and A. Elsaid, "Securing Financial Transactions with a Robust Algorithm: Preventing Double-Spending Attacks," *Computers*, vol. 12, no. 9, p. 171, Aug. 2023, doi: 10.3390/computers12090171.

[76] P. Zielonka *et al.*, "Stress Relaxation Behaviour Modeling in Rigid Polyurethane (PU) Elastomeric Materials," *Materials*, vol. 16, no. 8, p. 3156, Apr. 2023, doi: 10.3390/ma16083156.

[77] A. Galligan *et al.*, "Increased Thyroidal Activity on Routine FDG-PET/CT after Combination Immune Checkpoint Inhibition: Temporal Associations with Clinical and Biochemical Thyroiditis," *Cancers*, vol. 15, no. 24, p. 5803, Dec. 2023, doi: 10.3390/cancers15245803.

[78] P. Marinova *et al.*, "Synthesis, Characterization, and Antibacterial Studies of New Cu(II) and Pd(II) Complexes with 6-Methyl-2-Thiouracil and 6-Propyl-2-Thiouracil," *Appl. Sci.*, vol. 13, no. 24, p. 13150, Dec. 2023, doi: 10.3390/app132413150.

[79] G. Venitourakis *et al.*, "Neural Network-Based Solar Irradiance Forecast for Edge Computing Devices," *Information*, vol. 14, no. 11, p. 617, Nov. 2023, doi: 10.3390/info14110617.

[80] J. Ližbetin and J. Pečman, "Possibilities of Using Bluetooth Low Energy Beacon Technology to Locate Objects Internally: A Case Study," *Technologies*, vol. 11, no. 2, p. 57, Apr. 2023, doi: 10.3390/technologies11020057.

[81] M. Zhang, M. Li, L. Guo, and J. Liu, "A Low-Cost AI-Empowered Stethoscope and a Lightweight Model for Detecting Cardiac and Respiratory Diseases from Lung and Heart Auscultation Sounds," *Sensors*, vol. 23, no. 5, p. 2591, Feb. 2023, doi: 10.3390/s23052591.