Neurocomputing 579 (2024) 127415

Contents lists available at ScienceDirect

Neurocomputing

journal homepage: www.elsevier.com/locate/neucom

Trustworthy Artificial Intelligence -based federated architecture for symptomatic disease detection

Raúl López-Blanco [a,*], Ricardo S. Alonso [b,c], Sara Rodríguez-González [a], Javier Prieto [a], Juan M. Corchado [a,b]

[a] BISITE Research Group, University of Salamanca, Edificio I+D+i, Calle del Espejo 2, Salamanca, 37007, Castile and León, Spain
[b] AIR Institute - Deep tech lab IoT Digital Innovation Hub, Paseo de Belén 9A, Valladolid, 47011, Castile and León, Spain
[c] UNIR, International University of La Rioja, Av. de la Paz, 137, Logroño, 26006, La Rioja, Spain

ARTICLE INFO

Keywords:
Trustworthy Artificial Intelligence
Federated learning
Internet of Things
Healthcare
COVID-19

ABSTRACT

The recent viral outbreaks have had a significant impact on interpersonal relationships, particularly in enclosed spaces. Detecting and preventing the transmission of diseases such as COVID-19 has become a top priority. These diseases are typically identifiable through the symptoms they cause in humans. However, the collection of personal and health data for use in Artificial Intelligence models can give rise to ethical, security, and privacy issues. Therefore, it is necessary to have architectures that maintain the principles of Trustworthy Artificial Intelligence by design. This work proposes a decentralised architecture based on Federated Learning for symptomatic disease detection using the edge computing paradigm, storing the information in the device that collected it, and the foundations of Trustworthy Artificial Intelligence. The architecture is designed to be robust, secure, transparent, and responsible while maintaining data privacy. The proposed approach can be used with medical information capture systems with different user profiles.

1. Introduction

Pandemics are one of the biggest problems of the globalised world, as demonstrated by the spread of the SARS-CoV-2 virus, which caused the global coronavirus pandemic [1]. In just four months since the first case, the disease has been reported in 181 countries and infected more than one million people [2]. Coronavirus disease was the leading cause of death worldwide in December 2020, surpassing other causes such as heart attacks and cancer [3].

New technologies have facilitated the collection and handling of patient data, making it much more efficient to determine the number of infections and to collect other valid data for statistics and for building mathematical models to predict their evolution [4]. However, improvements can be made in the management and collection of data for other pandemic situations [5].

Data capture is becoming more and more widespread thanks to the growing use of IoT devices in different sectors [6,7] and finding its way more and more towards the Smart City concept [8,9]. However, it is increasingly difficult to share this data due to privacy restrictions on personal data and even more so on health data. It is essential that there is a relationship of trust with the entity that stores the data [10].

Until now, artificial intelligence models have been trained using large datasets from different sources that have been merged into one to facilitate the training of these models. However, such practices have begun to be questioned due to the ethical and security implications they raise [11].

This type of questioning is even more pronounced when it comes to medical data, which, due to its implications, is specifically protected by the European Parliament's Directive (EU) 2016/680 [12]. How to share medical data and how technology can help in this process has been widely discussed [13]

De-identification is one of the processes that have been used so far to make data sharing safer and more reliable for the owners of the data. This process consists of removing personal data associated with other data that can be used for studies and/or statistics. [14].

In recent years, in response to the problem of pooling and massively sharing data to train Artificial Intelligence models, a number of techniques have emerged that allow these models to be trained in a more reliable, secure, responsible and even sustainable way [15].

There are two trends when it comes to the generation of artificial intelligence models, one is to maintain the security of the datasets while preserving the privacy of the entity generating them; in response to this, Federated Learning has emerged [16], which allows the training of models in a distributed way from the aggregation of locally

* Corresponding author.
E-mail address: raullb@usal.es (R. López-Blanco).

https://doi.org/10.1016/j.neucom.2024.127415
Received 1 February 2023; Received in revised form 12 January 2024; Accepted 17 February 2024
Available online 28 February 2024

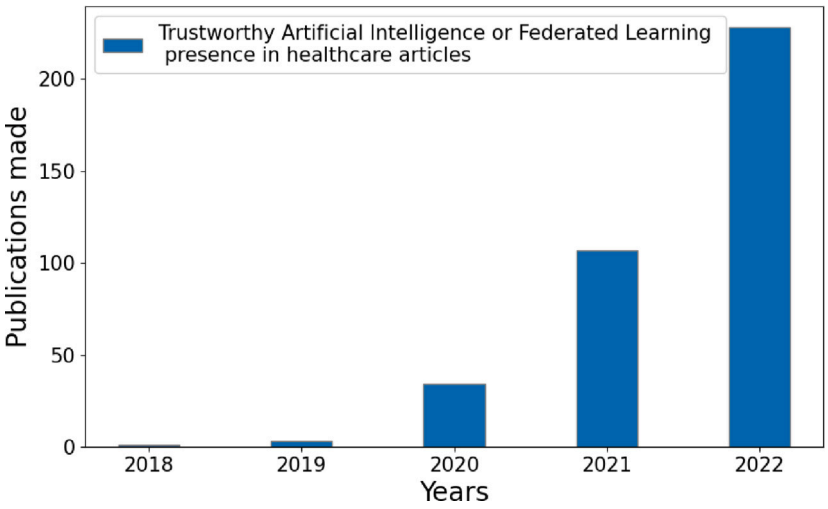

Fig. 1. Trustworthy Artificial Intelligence and Federated Learning appearances in healthcare papers. *Source:* Data retrieved from Scopus®(January 28th, 2023).

trained pieces of the model. The other need observed in this field is to achieve reliable and explicable models [17], capable of maintaining a sufficiently stable ethical framework so that the incorporation of these models in different sectors and aspects of everyday life is centered on people.

The areas where the need to develop artificial intelligence models has grown the most are those where decision-making is more critical, such as in autonomous driving [18], or where data is more private, such as in the field of health [19]. In the latter, the number of scientific publications using AI has grown from just 500 in the early 2000s to almost 4000 in 2019 [20].

This new dimension of AI, federated learning and model trustworthiness is gaining traction (see Fig. 1) in healthcare. To maintain this ethical framework for healthcare data, it is necessary to provide architectures and models that uphold this principle of trustworthiness and security. This article proposes an architecture designed for distributed training of models based on data collected by biometric access control devices [21].

The rest of the article is structured as follows: Section 2, which includes related work and relates federated learning and Trustworthy AI to the healthcare sector. Section 3 presents the architecture presented in this article and explains its components. Finally, Section 4 discusses the conclusions and future research directions.

2. Related works

This section highlights work related to the current work that has contributed to the creation of data sharing and model training architectures for health-related settings.

The first studies that have been used to understand the status of federated learning in the health sector have been the systematic reviews proposed by Antunes et al. [22] and the one proposed by Nguyen et al. [23]. The first is based on an understanding of the current use of federated learning for Electronic Health Records (EHR) management and proposes a knowledge-based architecture. The second makes a more global review of the applications that FL is having in the world of health. Both help to put the spotlight on studies that present federated learning architectures and models.

Among the studies reviewed, some focus on the management of EHRs, such as the one carried out by Liu et al. [24] to improve the classification of these medical records through deep learning models using federated architectures, where the nodes are the hospital complexes that generate data.

Other architectures, such as the one proposed by Passerat-Palmbach et al. [25], use other technologies, such as blockchain, to ensure privacy in the model aggregation processes and security in user authentication.

In addition to architectures, frameworks stand out, which are the majority of the works reviewed. The first of these frameworks is along the same lines as Passerat-Palmbach's architecture. The work by Singh et al. [26] exposes the need to preserve the privacy of each node and uses blockchain and cloud computing for the aggregation of the parts of the partial models.

Among the frameworks reviewed is that of Tedeschini et al. [27], which analyses different federated learning methods using the Message Queuing Telemetry Transport (MQTT) protocol for data transfer. The paper by Yuan et al. [28] extends this type of learning to all types of IoT devices in healthcare. The work by Silva et al. [29] exposes a framework as an interface for visualising data about what is happening in the network of federated nodes. All three papers pay little attention to privacy and process security.

Finally, it is also worth highlighting the work of Raza et al. [30], which, although based more on transfer learning, achieves very good results and directs its future lines of work towards federated learning (see Table 1).

Whether they are frameworks or federated architectures, they tend to model the healthcare sector as a set of data-generating nodes (hospitals, IoT devices), which provides privacy by construction of the architecture. However, the other aspects that make models, architectures and frameworks trustworthy (robustness, generalisability, explainability, transparency, reproducibility, fairness) are rather secondary, always giving priority to the efficiency of the models, architectures and frameworks.

Upon review of the works, it is clear that both architectures and frameworks have deficiencies, particularly in latencies (such as the use of blockchain networks or edge computing), security, and reliability. Therefore, this article focuses on designing a federated architecture based on reliability.

3. Architecture proposal

This section presents the proposed architecture, which is based on the foundations of federated learning, which distributes the computation in the learning tasks, and is based on the pillars of trustworthy AI to obtain a legal, ethical and robust architecture. This experimental architecture is called FBAC (Federated Biometric Access Control).

The architecture comprises nodes, which are medical devices capable of collecting information from various sensors, processing it, and

Table 1
Related works reviewed that use FL in healthcare.

Related works	Topic	Key contributions	Limitations
[24]	FL-based architecture for EHR management	Enhances FL architectures through deep learning	Few details on evaluation process
[25]	Distributed Federated Learning architecture with blockchain	Secure data privacy-preserving aggregation protocol	There is no information on the performance of the blockchain network or the latencies it may cause
[26]	Federated Learning architecture with blockchain	Blockchain and Federated Learning-enabled Secure Architecture for Privacy-Preserving in Smart Healthcare	Cloud computing may include unacceptable latencies
[27]	Real-time distributed framework based on MQTT	Analysis of different FL methods and framework for distributed networks	Does not provide information on the trustworthiness of the architecture
[28]	Advanced federated learning framework	Advanced federated learning framework	The IoT devices privacy has not been a priority
[29]	Open-source federated learning frontend framework	DFramework is stable in communication, while being robust	Data on the trustworthiness of training should be provided
[30]	FL Framework in for ECG-based healthcare using explainable artificial intelligence	Framework outperforms other classifiers, offers explainability and efficiency	The architecture is not based on federated learning as such but uses a centralised database

storing it locally. The name server node acts as a registry, noting which node has which information and the transfers of this information. Fig. 2 illustrates the architecture's structure. The process is as follows:

- **Step 1**. A node, **N**, requests data from the name server for known users who have passed through it to retrain its local model. **N** also informs the name server of any new information it has.
- **Step 2**. The name node informs **N** which node(s) have information about the user(s) it is inquiring about.
- **Step 3** and **4**. These steps establish communication between nodes that need to share information. Two types of information can be shared:
  - Encrypted and de-identified user data, which is used to train models locally.
  - Hyperparameters of the models, which are used to adjust locally trained models either from specific users or as a method of readjusting the generic model.

We now turn to comment the foundations on which the architecture is based and how it implements each of them to become a reliable alternative to other federated architectures already existing in the literature. These foundations have been extracted from the article by Li et al. [31] and the European Commission's Ethical Guidelines for Trustworthy AI [32] guide:

- **Robustness.** It is considered as the ability of the system to avoid erroneous data, which directly affects performance. In the proposed architecture, the occurrence of erroneous data has been made more difficult in several ways. Firstly, the data obtained by each of the sensors are not considered definitive until the sensor measurement reaches a percentage of accuracy of 80%, in addition to this the sensor performs several measurements within the time window and compares them to avoid extreme values or peaks that do not correspond to reality. Another element is the face recognition that has been realised with convolutional networks and prevents any prediction or training process from being carried out without having recognised a face. In addition to this active protection, there is also a reactive protection that checks the historical data series for numerical anomalies. If a data set is marked as suspicious, it does not become part of the training sets, in order to avoid algorithmic distortions.
- **Generalisation.** It represents the ability to distil knowledge from limited training data to make accurate predictions about unseen data. In this case, the model trains on a dataset as large as the number of users in the system, but only has three types of data and low variance, which makes the generalisation process and even the knowledge transfer process very easy.
- **Transparency.** It considers AI as a computer system and aims to disseminate information about its entire life cycle. It is guaranteed by design in this architecture. First by the type of computing chosen for the devices, which only compute at the edge, therefore, user information is only shared among the network of devices and is never transferred to the cloud. The data of each user is stored only for the purpose of improving the overall system algorithm and each user's own algorithm.
- **Reproducibility.** Computational procedures to verify AI research. Although this factor could be seen more clearly in tests with real data sets, it is true that the components of the architecture and its operation have been explained during this work, which allows its operation to be reproduced in order to verify its reliability.
- **Fairness.** An algorithm is fair if its results are independent of a certain set of variables that we consider sensitive and unrelated to it. In this case the sensitive data can be the face, personal data and medical data captured from each user. In this case, fairness is guaranteed, since the algorithm only trains with the de-identified data, i.e. they are independent at the training level of the person from whom they were captured.
- **Privacy Protection.** Privacy protection mainly refers to the protection against unauthorised use of data that can directly or indirectly identify a person or household. In addition to the de-identification processes discussed above, the data is encrypted in the database of each device and thus travels between nodes, only being decrypted at the destination, preventing the data from being leaked to third parties outside the architecture.

The architecture is composed of several elements that perform the data capture, the distribution of data in a structured way among the different nodes and the local training processes that take place in each of the nodes in order to aggregate them in the global models.

3.1. Node

Each of the devices has a series of sensors capable of collecting information from the user before he/she enters an enclosed public space. Firstly, it has two tablets at different heights, which improves accessibility, and which are responsible for identifying, by means of their cameras, when a user is in front of the device.

After this, the measurement process begins, which is carried out by means of a sensor that measures pulse oximetry and another that measures temperature. The information collected by these sensors is stored locally in each device, waiting to start a new phase of information exchange with the central Name Server.

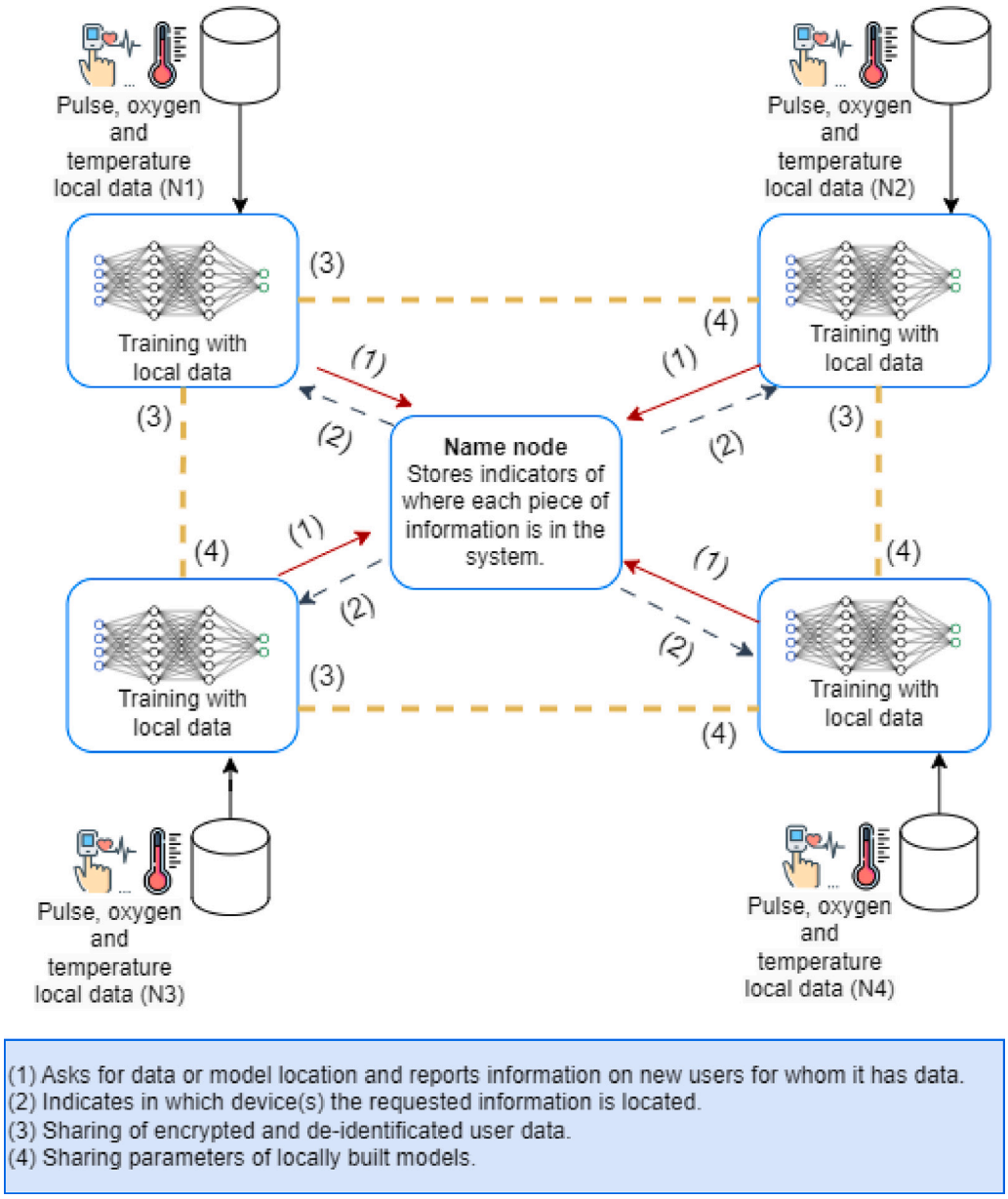

Fig. 2. FBAC (Federated Biometric Access Control) Architecture deployed in this work.

These nodes are located in public places and allow or deny access to the user depending on the captured vital signs, in the case of symptomatic detection of a possible disease, entry will be denied, if the captured vital signs are normal, entry is allowed.

3.2. Name server

This node has the function of coordinating which data should be transferred between which nodes. It has two separate registers, one which stores the information that each node has in its local database, divided into information from identified and unidentified users; the other register stores the models that each node has in its local cache (see 3).

The information collected from each user, whether known or unknown, is used to train the global model of the system by means of local partial training. The parameters of each of these local models are shared with the rest of the nodes in the architecture in update rounds decided by the nodes themselves when they consider that they have important updates with respect to the previously trained versions.

In the case of a known user who regularly uses the devices to access public places, his or her information is stored until there is a sufficient dataset to create a personalised model for him or her. If other devices in the network have information about the same user, the node with more data will be asked by the node with less data to speed up communication and use this data to train the personalised model.

3.3. Architecture components communication

Assuming that the architecture is composed of a set of $F = \{1, \ldots, N\}$ nodes, where each device is $d \in F$. Each device collects data about its

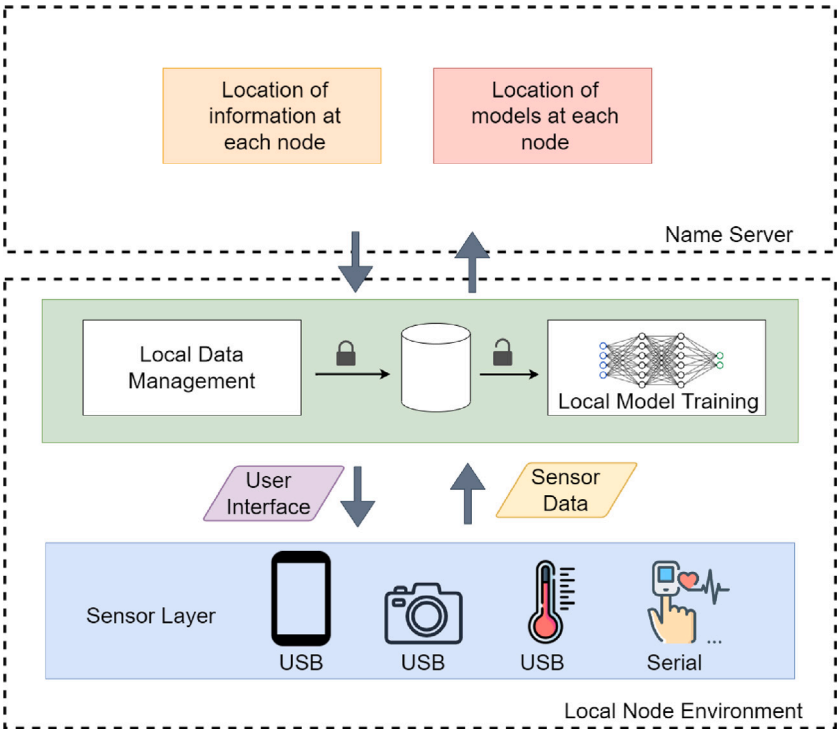

Fig. 3. Composition of the nodes structuring the proposed architecture.

users with the aim of making customised models locally, but with data received from the rest of the nodes and all of them have in common the generic model that can be parameterised by the vector $\theta \in \mathbb{R}^{dx1}$. The objective pursued by all nodes in the network is the minimisation of Eq. (1)

$$P(0) : \underset{\theta}{Minimize} \qquad F(\theta) \triangleq \frac{1}{N} \sum_{d \in F} f_i(\theta) \tag{1}$$

Furthermore, Eq. (1) reflects an important aspect of machine learning: the smoothness of a loss function. This metric indicates the rate at which the function changes in response to changes in its inputs. A smooth loss function has derivatives (gradients) that change gradually, which helps to stabilise the learning process by facilitating its minimisation.

In federated architectures, minimising this function is particularly important because communication between nodes is limited for performance reasons, which can slow down model convergence. Smoothness ensures that small differences in data between nodes do not result in large variations in computed gradients. This is crucial when nodes update their models locally and then share them with other nodes.

Using components such as nodes and a name server, it is possible to eliminate the need for a central hub node where the generic model of the entire system is trained. By employing the type of communication described, the computation capacity of the nodes is utilised to train both the local and generic models, with the name server serving as a registry of transactions and information locations. If the name node goes down, a recovery mechanism can be established because all nodes know what they store and with whom they have shared the information. No changes in content have been made.

Knowing already the robustness and reliability of the architecture, the two use cases about the communication that can occur when new users are detected on the platform, whether it is a known or unknown user, are presented in Fig. 4 and Fig. 5.

3.4. Numerical analysis of FBAC architecture

As the final point in presenting the architecture, we will perform a small theoretical analysis using a fictitious scenario with four nodes, $F = \{N_1, N_2, N_3, N_4\}$, and a name server, NS, deployed as shown in Fig. 2. Assuming an idle state of the system, there is a node, N_1, that wants to send the information it has received about the users during the day, and a node, N_2, that wants to retrieve user information that has passed through N_1.

In the system, x represents all the information about a user U. Let us consider the time it would take for x to travel to N_2. Technical term abbreviations are explained when first used. Two variables are set for this purpose: T_{send}, which is the time it takes to send information between two nodes, and T_{NS}, which is the time it takes to communicate with the name server, being always $T_{send} \gg T_{NS}$ since in the first one we send data and in the second one there is only a question-answer process. Eq. (2) shows the total time T required for sending this information.

$$T = 2T_{NS} + T_{send} \tag{2}$$

If a central node T_{send} were used instead of a name server, it would be multiplied by the number of nodes that need to share information simultaneously. This makes the approach much more appealing in this scenario.

Another important metric is resilience which indicates the probability of maintaining connectivity in the face of failures and could be modeled as failed nodes versus total nodes, but will be done as seen in Eq. (3), since the failure of a node is not relevant as long as it has shared its information with another node.

$$R = 1 - \frac{Lost\ Information}{Total\ Information} \tag{3}$$

The information of an authenticated user in the system would only be lost if they pass through a certain number of nodes, which crash and lose their information. The probability of a user passing through a single future failed node decreases as the number of nodes increases. Therefore, resilience and scalability are interconnected in this architectural approach.

4. Conclusions

Although the architecture presented in this work has not been tested in an experimental scenario, it is possible to draw several conclusions

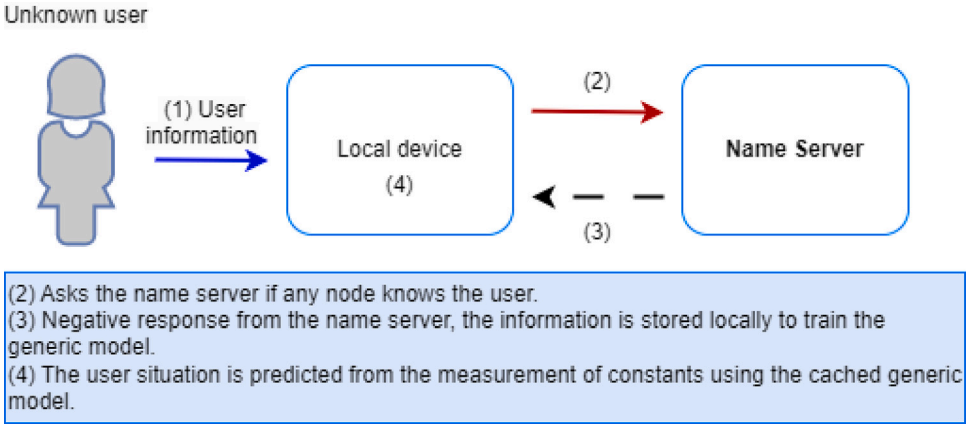

Fig. 4. Architecture communicative processes when an Unknown user is detected.

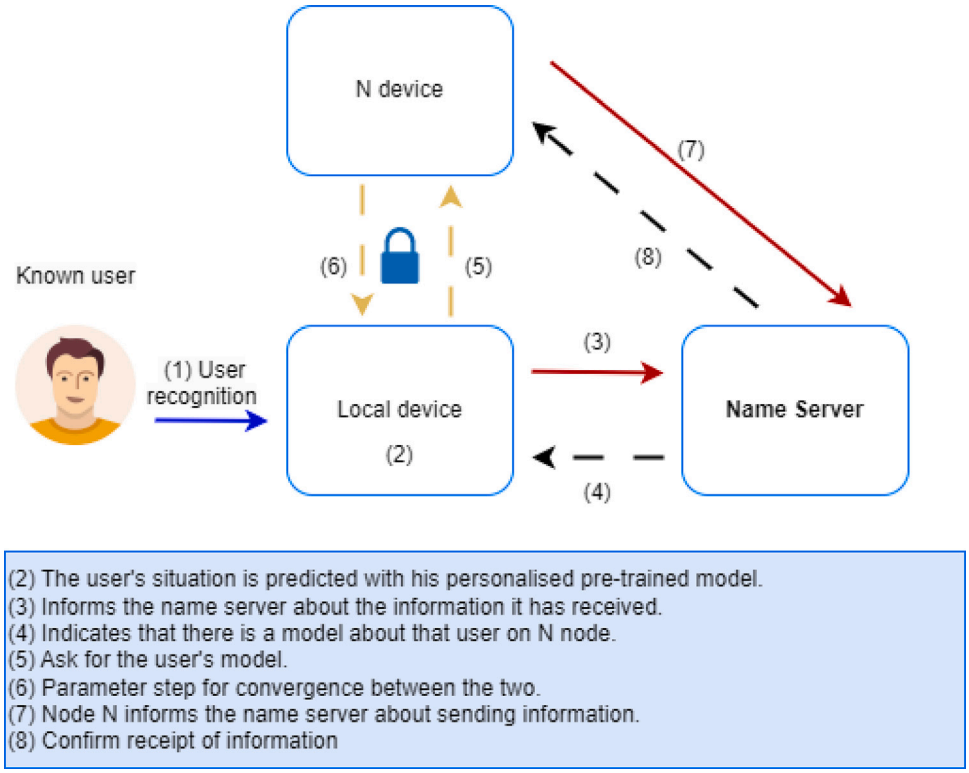

Fig. 5. Architecture communicative processes when an Known user is detected.

related to its construction and applicability in scenarios such as the medical field, where reliable data capture and AI models are required. The Section 3 presents evidence of the architecture's robustness.

In data capture, an accuracy threshold is implemented in the sensor reading and time windows are used to avoid spikes in the measurements. Additionally, the historical series are reviewed to identify anomalies that may affect training. We work with a reduced dataset, both in variance and in number. The potential issue of generalisation is not a problem for AI models, as they tend to generalise better due to the lower complexity and variability in the data. The use of edge computing ensures that user data remains within a controlled network of devices, improving the confidentiality and transparency of data handling. Additionally, the storage of data for algorithm improvement respects user privacy.

The detailed description of the FBAC architecture components and their operation provides a solid basis for replication and reliability verification. The strategy of training with de-identified data is key to ensuring fairness in the algorithms. By eliminating sensitive and personal variables in the training process, the risk of unfair bias is reduced and algorithmic fairness is promoted. Additionally, the use of de-identified data promotes privacy protection. The storage and sharing of information between nodes reduces the risk of data leaks and unauthorised use, in line with data protection and privacy regulations. In healthcare, privacy is critical and must be kept that way.

For all the characteristics mentioned in this section, FBAC is considered a robust architecture by construction. It promotes generalisation, data transparency for users, reproducibility, fairness during training processes, and privacy protection during data persistence and transport. Regarding future work, it is presented as follows:

- A validation process of the proposed architecture is necessary to ensure its operational processes and efficiency, which is considered as a future line of work. For this process, each device will be configured as a network node and the network will be provided with a central name server.

- Explainability is another of the pending points of this architecture and it is necessary to develop algorithms that, in addition to symptomatically detecting diseases, provide an explanation that can be used by medical personnel to understand the decisions of the model.

CRediT authorship contribution statement

Raúl López-Blanco: Formal analysis, Investigation, Writing – original draft, Writing – review & editing. **Ricardo S. Alonso:** Investigation, Resources, Supervision, Validation, Writing – original draft, Writing – review & editing. **Sara Rodríguez-González:** Investigation, Methodology, Project administration, Validation. **Javier Prieto:** Conceptualization, Supervision, Validation, Formal analysis. **Juan M. Corchado:** Funding acquisition, Project administration, Supervision.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Raúl López Blanco reports a relationship with University of Salamanca that includes: employment. Raúl López Blanco has patent Trustworthy Artificial Intelligence -based Federated Architecture for symptomatic disease detection.

Data availability

No data was used for the research described in the article.

Acknowledgments

This research has been partially supported by the Spanish Ministry of Science and Innovation under the RESILIENCE project (CNS2022-135101, MCIN/AEI /10.13039/501100011033) and by the European Union NextGenerationEU/PRTR.

References

[1] M. Perez-Bermejo, M.T. Murillo-Llorente, The fast territorial expansion of the Covid-19 in Spain, J. Epidemiol. (2020) JE20200123.
[2] A. Hoseinpour Dehkordi, M. Alizadeh, P. Derakhshan, P. Babazadeh, A. Jahandideh, Understanding epidemic data and statistics: A case study of COVID-19, J. Med. Virol. 92 (7) (2020) 868–882.
[3] H.K. Koh, A.C. Geller, T.J. VanderWeele, Deaths from COVID-19, JAMA 325 (2) (2021) 133–134.
[4] L.F. Castillo Ossa, P. Chamoso, J. Arango-López, F. Pinto-Santos, G.A. Isaza, C. Santa-Cruz-González, A. Ceballos-Marquez, G. Hernández, J.M. Corchado, A hybrid model for COVID-19 monitoring and prediction, Electronics 10 (7) (2021) 799.
[5] N. Shadbolt, A. Brett, M. Chen, G. Marion, I.J. McKendrick, J. Panovska-Griffiths, L. Pellis, R. Reeve, B. Swallow, The challenges of data in future pandemics, Epidemics (2022) 100612.
[6] M.E. Pérez-Pons, M. Plaza-Hernández, R.S. Alonso, J. Parra-Domínguez, J. Prieto, Increasing profitability and monitoring environmental performance: A case study in the agri-food industry through an edge-IoT platform, Sustainability 13 (1) (2020) 283.
[7] R. Casado-Vara, F.D.l. Prieta, S. Rodriguez, J. Prieto, J.M. Corchado, Cooperative algorithm to improve temperature control in recovery unit of healthcare facilities, in: International Symposium on Distributed Computing and Artificial Intelligence, Springer, 2018, pp. 49–62.
[8] P. Chamoso, A. González-Briones, S. Rodríguez, J.M. Corchado, Tendencies of technologies and platforms in smart cities: a state-of-the-art review, Wirel. Commun. Mob. Comput. 2018 (2018).
[9] J.M. Corchado, P. Chamoso, G. Hernández, A.S.R. Gutierrez, A.R. Camacho, A. González-Briones, F. Pinto-Santos, E. Goyenechea, D. García-Retuerta, M. Alonso-Miguel, et al., Deepint. net: A rapid deployment platform for smart territories, Sensors 21 (1) (2021) 236.
[10] R. Casado-Vara, J. Corchado, Distributed e-health wide-world accounting ledger via blockchain, J. Intell. Fuzzy Systems 36 (3) (2019) 2381–2386.
[11] R. Shokri, V. Shmatikov, Privacy-preserving deep learning, in: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015, pp. 1310–1321.
[12] European Parliament and The European Council, Directive (EU) 2016/680 of the European parliament and of the council of 27 april 2016, on the protection of natural persons with regard to the processing of personal, Off. J. Eur. Union 119 (2016) 89–131.
[13] H. Jin, Y. Luo, P. Li, J. Mathew, A review of secure and privacy-preserving medical data sharing, IEEE Access 7 (2019) 61656–61669.
[14] J. Gardner, L. Xiong, HIDE: an integrated system for health information DE-identification, in: 2008 21st IEEE International Symposium on Computer-Based Medical Systems, IEEE, 2008, pp. 254–259.
[15] T. Yigitcanlar, R. Mehmood, J.M. Corchado, Green artificial intelligence: Towards an efficient, sustainable and equitable technology for smart cities and futures, Sustainability 13 (16) (2021) 8952.
[16] R.S. Alonso, J. Prieto, F. de La Prieta, S. Rodríguez-González, J.M. Corchado, A review on deep reinforcement learning for the management of SDN and NFV in edge-IoT, in: 2021 IEEE Globecom Workshops, GC Wkshps, IEEE, 2021, pp. 1–6.
[17] J.M. Corchado, S. Ossowski, S. Rodríguez-González, F. De la Prieta, Advances in explainable artificial intelligence and edge computing applications, Electronics (ISSN: 2079-9292) 11 (19) (2022) http://dx.doi.org/10.3390/electronics11193111, URL https://www.mdpi.com/2079-9292/11/19/3111.
[18] K. Dev, Y. Xiao, T.R. Gadekallu, J.M. Corchado, G. Han, M. Magarini, Guest editorial special issue on green communication and networking for connected and autonomous vehicles, IEEE Trans. Green Commun. Netw. 6 (3) (2022) 1260–1266.
[19] R. Casado-Vara, F. De la Prieta, S. Rodriguez, J. Prieto, J.M. Corchado, Cooperative algorithm to improve temperature control in recovery unit of healthcare facilities, in: Distributed Computing and Artificial Intelligence, Special Sessions II, 15th International Conference 15, Springer, 2020, pp. 49–62.
[20] Organisation for Economic Co-operation and Development's Directorate for Employment, Labour and Social Affairs and Directorate for Science, Technology and Innovation, Trustworthy AI in Health, OECD, 2020.
[21] R. López-Blanco, R.S. Alonso, J. Prieto, S. Rodríguez-González, J.M. Corchado, Indoor access control system through symptomatic examination using IoT technology, fog computing and cloud computing, in: Hybrid Artificial Intelligent Systems: 17th International Conference, HAIS 2022, Salamanca, Spain, September 5–7, 2022, Proceedings, Springer, 2022, pp. 60–72.
[22] R.S. Antunes, C. André da Costa, A. Küderle, I.A. Yari, B. Eskofier, Federated learning for healthcare: Systematic review and architecture proposal, ACM Trans. Intell. Syst. Technol. 13 (4) (2022) 1–23.
[23] D.C. Nguyen, Q.-V. Pham, P.N. Pathirana, M. Ding, A. Seneviratne, Z. Lin, O. Dobre, W.-J. Hwang, Federated learning for smart healthcare: A survey, ACM Comput. Surv. 55 (3) (2022) 1–37.
[24] D. Liu, T. Miller, R. Sayeed, K.D. Mandl, FADL: Federated-autonomous deep learning for distributed electronic health record, 2018, arXiv preprint arXiv:1811.11400.
[25] J. Passerat-Palmbach, T. Farnan, R. Miller, M.S. Gross, H.L. Flannery, B. Gleim, A blockchain-orchestrated federated learning architecture for healthcare consortia, 2019, arXiv preprint arXiv:1910.12603.
[26] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, B. Yoon, A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology, Future Gener. Comput. Syst. 129 (2022) 380–388.
[27] B.C. Tedeschini, S. Savazzi, R. Stoklasa, L. Barbieri, I. Stathopoulos, M. Nicoli, L. Serio, Decentralized federated learning for healthcare networks: A case study on tumor segmentation, IEEE Access 10 (2022) 8693–8708.
[28] B. Yuan, S. Ge, W. Xing, A federated learning framework for healthcare iot devices, 2020, arXiv preprint arXiv:2005.05083.
[29] S. Silva, A. Altmann, B. Gutman, M. Lorenzi, Fed-biomed: A general open-source frontend framework for federated learning in healthcare, in: Domain Adaptation and Representation Transfer, and Distributed and Collaborative Learning: Second MICCAI Workshop, DART 2020, and First MICCAI Workshop, DCL 2020, Held in Conjunction with MICCAI 2020, Lima, Peru, October 4–8, 2020, Proceedings 2, Springer, 2020, pp. 201–210.
[30] A. Raza, K.P. Tran, L. Koehl, S. Li, Designing ecg monitoring healthcare system with federated transfer learning and explainable ai, Knowl.-Based Syst. 236 (2022) 107763.
[31] B. Li, P. Qi, B. Liu, S. Di, J. Liu, J. Pei, J. Yi, B. Zhou, Trustworthy ai: From principles to practices, ACM Comput. Surv. 55 (9) (2023) 1–46.
[32] European Commission and Directorate-General for Communications Networks, Content and Technology, Ethics Guidelines for Trustworthy AI, Publications Office, 2019, http://dx.doi.org/10.2759/346720.