

A Federated Learning System with Biometric Medical Image Authentication for Alzheimer's Diagnosis

Francesco Castro^a, Donato Impedovo^b and Giuseppe Pirlo^c
Univeristy of Bari Aldo Moro, Via E. Orabona, 4, Bari, 70125, Italy


Keywords: Federated Learning, Alzheimer's Disease, Medical Image, Data Poisoning, Secure Healthcare System.


Abstract: There are concerns within the medical/scientific community about the use of machine learning models for disease diagnosis from medical images. The causes are related not only to the high performance required in models for disease diagnosis but also to the sensitivity of the data processed and the protection of patient privacy. There are stringent policies on medical image dissemination to prevent image theft, image de-anonymization, data poisoning attacks, and other security issues. The proposed system for AD diagnosis from RGB MRI brain images implements the Federated Learning (FL) architecture and a strategy of medical image authentication through biometric recognition to protect the privacy and confidentiality of the medical image used for the training model and to mitigate the data poisoning attacks on the model. Experiments conducted on two datasets of RGB MRI images (OASIS and ADNI) demonstrate that the proposed system achieved performance comparable to a centralized ML system without a privacy-preserving strategy. The proposed system represents a solution to solve security and privacy issues in a healthcare application for AD diagnosis.


1 INTRODUCTION

Alzheimer's disease (AD) is a neurodegenerative disease that affects the nerve cells within the brain, progressively leading to irreversible cognitive decline. Common symptoms of AD are to be found in memory loss, cognitive decline, and changes in personality and behavior. AD is one of the most common neurodegenerative diseases, and it is estimated that by 2050, one in 85 people will be affected by AD (Wang et al., 2018). AD is incurable, but an early diagnosis would allow a slower decline of the disease, leading to significant benefits for affected individuals (Angelillo, Balducci, et al., 2019; Ghosh et al., 2023a). Several methodologies are used to detect AD, such as Magnetic resonance imaging (MRI), computer tomography (CT), positron emission tomography (PET), and behavioral biometrics through Human Activity Recognition (HAR) (Angelillo, Impedovo, et al., 2019; Cicirelli et al., 2022; Vincenzo Dentamaro et al., 2021; Gattulli et al., 2022; Gattulli, Impedovo, Pirlo, & Sarcinella, 2023; Gattulli, Impedovo, Pirlo, & Semeraro, 2023;

Impedovo et al., 2012; Salehi et al., 2020). MRIs have been increasingly used to diagnose AD through machine learning (ML) methods. Among the ML methods, Convolutional Neural Networks (CNN) are the most promising and commonly used approaches (Wen et al., 2020), (Cheriet et al., 2023). However, using ML in healthcare involves several significant risks to security and privacy (Sivan & Zukarnain, 2021). On the other hand, medical imbalanced data affects the performance of ML diagnostic systems (Vincenzo Dentamaro et al., 2018). For this reason, these technologies have difficulty becoming a standard in healthcare applications. Wrong or improper use of these tools in healthcare would lead to disastrous consequences that could even cost people's lives. Some of the most critical issues related to user privacy and security are constraining policies on medical image dissemination, lack of data for optimal model learning, interception attacks, de-anonymization attacks, data poisoning attacks, malware attacks, lack of transparency, and any type of anomalies (Cannarile et al., 2022; Carrera et al., 2022; V. Dentamaro et al., 2021).

^a  <https://orcid.org/0000-0002-8579-8941>

^b  <https://orcid.org/0000-0002-9285-2555>

^c  <https://orcid.org/0000-0002-7305-2210>

Federated learning (FL) represents a promising technique to mitigate some of these issues (Li, Wen, et al., 2021). FL enables decentralized learning by preventing healthcare institutions from sharing their data externally. The institutions participate in the training of a global model and receive the knowledge learned from the data of all institutions. The basic idea is to train a local model with local data for each healthcare institution and share only the local model parameters. A global model receives and updates its parameters with the local parameters of each organization through different strategies. Finally, the updated global model is shared with all the organization's participants. Therefore, FL is a privacy-preserving approach to compliance with GDPR requirements and encourages healthcare institutions to share knowledge acquired from their data while maintaining confidentiality. However, the FL approach is vulnerable to data poisoning attacks and other types of attacks related to ML algorithms (Mothukuri et al., 2021). Figure 1 shows some possible attacks in the FL system for healthcare applications. A data poisoning attack consists of inserting images that cause the system to learn incorrectly or, even worse, cause the system to give the desired output. In (CHAN-HON-TONG, 2018) an algorithm to perform an invisible data poisoning attack that compromises the prediction result of a deep learning model has been presented. Data poisoning attacks could have disastrous consequences in healthcare applications.

The proposed work presents an FL system to diagnose AD from RGB MRI's brain image, implementing a method of authenticating MRI images through physician biometric data to mitigate data poisoning attacks. The proposed method incorporates the fingerprint of the physician authorized to give input images for local model training within an RGB MRI image. The embedding is done with a digital watermarking technique using the Discrete Wavelet Transform (DWT) and the Singular Value Decomposition (SVD) that ensures the visual security image (Castro et al., 2023). The physician's fingerprint is extracted from the RGB MRI image for authentication before training the local model. In this way, only the authorized physicians can train the local model. Subsequently, the trained parameters of the local model are sent to the global model for FL.

Few state-of-the-art approaches have explored the use of FL in the context of AD diagnosis through MRIs (Ghosh et al., 2023b; Khalil et al., 2023), and none have addressed the problem of data poisoning

attacks. The main contributions of the proposed work are:

- Develop an FL system to diagnose AD from RGB MRI images, ensuring patient's privacy;
- Develop a methodology of RGB MRI image authentication to mitigate data poisoning attacks based on biometric recognition;
- Compare the proposed system performance with no-FL system performance to evaluate the trade-off between safety and performance.

2 RELATED WORKS

Several studies have shown the effectiveness of ML approaches for AD diagnosis from MRI images (Mirzaei & Adeli, 2022). Many studies have compared results obtained with deep learning approaches with shallow learning approaches. Deep learning techniques allow more accurate performance in recognizing AD, especially in the case of different stages of the disease (Suresha & Parthasarathy, 2020). Among the most recent ML approaches include enhanced probabilistic neural networks, neural dynamic classification, dynamic ensemble learning, and finite element machines. However, these approaches do not protect the privacy of medical images and patients. For this reason, FL systems have been developed for healthcare applications. FL approaches are used in contexts where data privacy is an essential requirement. Kaissis et al. highlight the great importance of using privacy protection techniques in learning systems that process medical images by presenting PriMIA (Kaissis et al., 2021). It is an open-source framework that implements learning neural networks on medical images by the FL method and uses prevention techniques for a de-anonymization and dataset reconstruction attack. PriMIA's focus is to protect sensitive data at every stage of learning while not sacrificing the performance of shared learning. FL is used in the healthcare domain for various tasks, such as brain tumors, mammograms, issues due to COVID-19, and more, as shown by Moon et al. (Narmadha & Varalakshmi, 2022). Interest in FL systems has involved institutions, government agencies, and multinational companies specializing in tech and IT. Nvidia has contributed to the release of Nvidia Flare, an SDK focusing on artificial intelligence and FL. In addition, Nvidia has released software specifically for applications in the medical field with MONAI

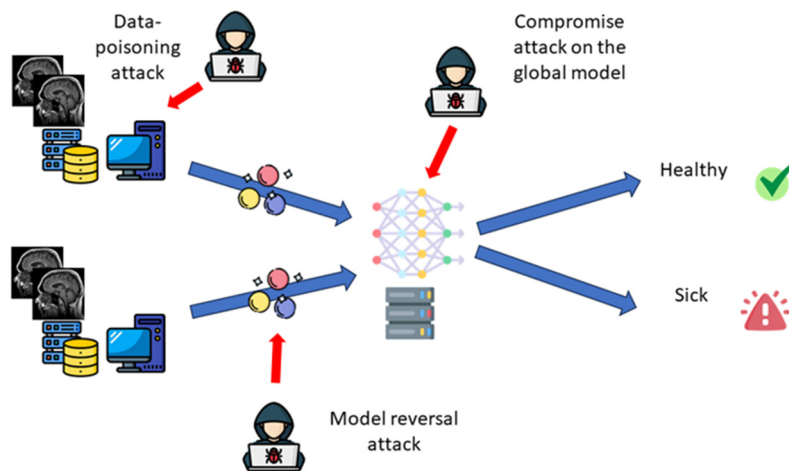


Figure 1: Vulnerabilities in the FL system.

(Medical Open Network for AI), on which FL systems can be implemented.

As well as a privacy-preserving approach, FL is also used to solve the problem of fragmentation of medical datasets. It results in low learning performance and poor generalization of ML models.

The performance obtained with the FL approach decentralized is similar to the performance of a centralized model. It thus shows how FL is a possible solution to the problem of dataset sparsity (Nguyen et al., 2022).

FL is used in both supervised and unsupervised learning. Bercea et al present FedDis (Bercea et al., 2022), an FL framework that aims to greatly simplify the work of clinicians by attempting to identify and segment abnormalities in brain MRIs that are part of the dataset. Labeling a dataset is arduous, and an unsupervised Autoencoder neural network was used to cluster the various MRIs produced by different healthcare institutions through FL.

Only a few studies have focused on FL approaches for AD recognition from MRI images (Ghosh et al., 2023b; Zhao & Huang, 2023). The accuracy and sensitivity of AD prediction with the FL approach are comparable with traditional ML approaches (Ghosh et al., 2023b).

Along with innumerable capabilities, FL has some critical issues related to data heterogeneity and ML attacks, such as reversal model and data poisoning attacks. Homomorphic encryption (HE) and secure multiparty computation (SMC) based on secret sharing have been proposed against reversal model attacks (Galantucci et al., 2021; Zhang et al., 2023).

(Li, He, et al., 2021) focus their studies on the issue of heterogeneous data used in FL, indicating how the diversification of these can lead to poor

performance of the model. They propose a method for locally correcting model updates by maximizing the representation similarity between local and global models. It has also been proposed as a valid method for resisting data poisoning attacks. Data poisoning is a relevant security issue in FL and ML algorithms. Data poisoning attacks compromise the final result or direct the model to a specific prediction, representing a significant issue, especially in health diagnostic systems. Han et al. propose a digital watermarking technique to prevent manipulation of the test medical images (Han et al., 2023). The technique is appropriate for medical images because it does not change important information in medical images and ensures privacy data. Digital watermarking can prevent image manipulation and ensure image authentication for the model training phase.

The proposed work presents an FL system to diagnose AD from RGB MRI images along with a method of authenticating MRI images through physician biometric data. Therefore, the proposed system ensures the privacy of medical images and their authentication against data poisoning attacks, thus making the system robust for use in real-world settings.

3 PROPOSED METHOD

The proposed system is based on the FL approach to ensure the privacy of medical images used in the training phase. The proposed system architecture is shown in Figure 2. Each medical institution trains the local model with local RGB MRI images. The local RGB MRI images are authenticated with the physician's fingerprint before local training to

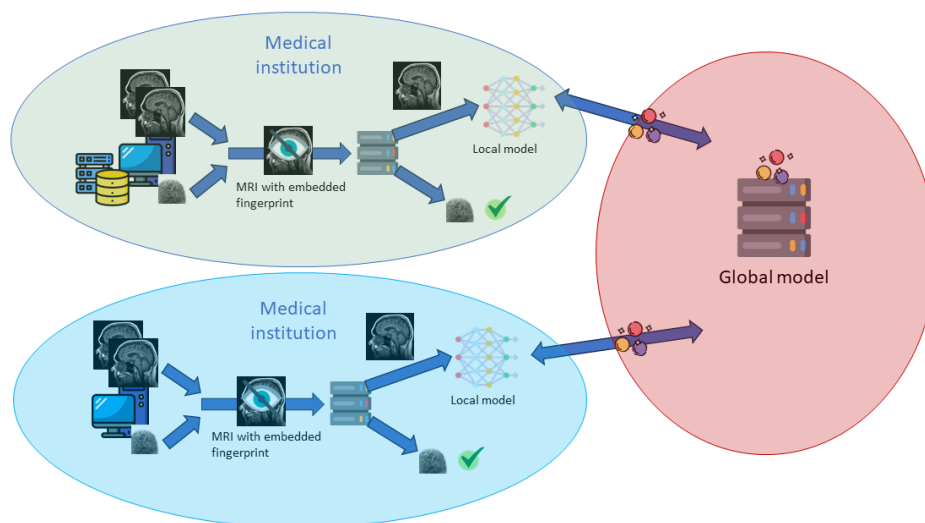


Figure 2: Proposed system architecture.

prevent data poisoning attacks. This stage is detailed in Section 3.1. Subsequently, the authenticated MRI images are used to train the local model, and the training parameters are sent to the central server. The central server aggregates the local parameters into a global model through the FedAvg strategy and sends the global model to each medical institution. The communication between medical institutions and the central server, the sending of parameters, the aggregation strategy, and the updating of the global model are detailed in Section 3.2. The architecture of the local model used for AD diagnosis is described in Section 3.3. The proposed system represents a strategy to implement an ML system for AD prediction with privacy protection and robustness to data poisoning attacks.

3.1 Preprocessing and Image Authentication Method

The preprocessing step includes embedding the physician's fingerprint to authenticate the MRI through a digital watermarking technique. The technique used is the Discrete Wavelet Transform (DWT), which consists of dividing the RGB MRI image into 4 sub-bands where each sub-band represents a specific image detail: horizontal (LH), vertical (HL), diagonal (HH), and approximation (LL). The LL sub-band is the coefficient matrix that contains the main image data. Figure 3 shows an RGB MRI image divided into the 4 sub-band through the DWT.

The LL sub-band cannot be changed, while the remaining sub-bands can be changed and replaced with other values to provide a visual secure

embedding. The embedding of the physician's fingerprint is performed by replacing the values of LH, HL, and HH with the fingerprint image factorization values. For the image factorization is used the Singular Value Decomposition (SVD) divides the image into 2 orthogonal matrixes U and VT) and 1 vector of singular values (S). Both DWT and SVD are common techniques of digital watermarking because they consist of invertible transformations. Therefore, it is possible to reconstruct the original image from the values obtained by transformations. The sub-band LH and HL are replaced with U and VT matrixes respectively. The values of vector S are inserted into the HH sub-band following through substitutions and permutations to introduce entropy into embedding and make it complex for an attacker to reconstruct the fingerprint image. Finally, the RGB MRI image with the embedding of the fingerprint image (watermarked image) is generated through the Inverse Discrete Wavelet Transform (IDWT) given as input LL and the replaced sub-bands. Figure 3 shows the results of the IDWT.

Figure 4 shows the visual security of the proposed method. The proposed method enables biometric authentication to be applied to the medical image used for model training. Therefore, the physician's fingerprint image is extracted from a watermarked image to authenticate the image before starting local model training, avoiding training with poisoned images. The extraction process involves applying DTW on the watermarked image to re-obtain the 4 sub-bands (LL' , LH' , HL' , and HH'). Consequently, LH' , HL' , and HH' contain the values of U, VT, and

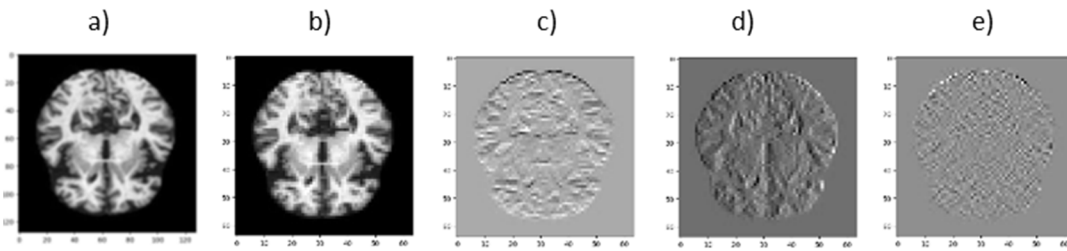


Figure 3: a) Original MRI image. b) LL of MRI image. c) LH of MRI image. d) HL of MRI image. e) HH of MRI image.

S respectively, used to reconstruct the fingerprint image through the SVD reconstruction. It consists of converting S into a diagonal matrix (D), and then the dot product between U, D, and VT is performed to obtain the image.

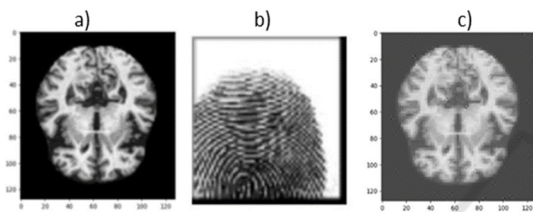


Figure 4: (a) original MRI image (b) fingerprint image (c) MRI image with embedding fingerprint (watermarked image).

3.2 Federated Learning

The proposed system is based on an FL architecture in which each medical institution participates in training the global model without sharing its patients' sensitive data. The entire process consists of 5 steps, as described below.

- Step 1: actors in the entire process are described, namely, the server and the various clients or nodes. The nodes participating in the federation are the hospitals or medical institutions that possess a database of RGB MRI images needed for AD prediction. The server owns the model to be trained that will be shared with the various participating nodes.
- Step 2: the server synchronizes with all nodes, sending the model base with null or random weights.
- Step 3: each node performs training of the newly received model with its local dataset of RGB MRI images.
- Step 4: the nodes only send the weights obtained during the learning phase to the server. The server performs the FedAvg aggregation approach of all the weights received to create a new model representing the learning performed by all the various nodes. The FedAvg combines

the local gradient computation assigned to each node with the gradient averaging computation performed by the server. On the other hand, the received weights are weighted according to the number of training examples of each node, and then the weights averaging is performed. FedAvg is robust to unbalanced and non-IDD distributions.

- Step 5: the server synchronizes with each node by sending the new version of the model and iteratively restarts the entire FL process.

The entire FL process is iterated several times by updating the global model at each iteration to allow the global model to learn the knowledge obtained from each node.

3.3 Convolutional Neural Network (CNN)

The model used for the training is based on a CNN, which is able to process RGB MRI images to detect significant patterns of the presence of AD. CNN has special convolutional layers, which can apply filters to the original image to recognize and extract patterns characteristic of the image. At a low level, thus considering the first few layers, the CNN applies convolutional filters to be able to recognize essential elements such as lines, angles, figures, etc., and then goes on to more and more complex elements that, at a high level, might be characteristic of those suffering from cognitive impairment due to AD such as more irregular and less defined grooves. To reduce the computational cost and choose the features with higher magnitude, CNN has layers for the Max Pooling technique, which consists of choosing the coefficient with a higher value within a submatrix of the input. This reduces the dimensionality of the image and favors the most significant features. The extracted features are given as input to a Flatten layer to reduce the dimensionality of the images. The last output layer is represented by a Dense layer of binary classification (disease or no disease), consisting of a single neuron with a sigmoidal activation function.

Summarizing the implemented CNN architecture is constituted by:

- two-dimensional convolutional input layer with Relu activation function;
- two Max Pooling layers;
- flatten layer;
- dense layer with a sigmoid activation function.

4 EXPERIMENTS

The proposed system is tested using two datasets of RGB MRI images to predict AD, as described in Section 4.1. Two scenarios have been simulated to evaluate the effectiveness of the proposed system compared to a traditional ML system. The first scenario implements a traditional ML system based on the CNN described in Section 3.3 where the medical institutions share the local RGB MRI images into a central database to train the model for AD prediction. This scenario presents vulnerabilities related to data privacy and data poisoning attacks. The second scenario implements the proposed system with FL architecture and RGB MRI image authentication. This scenario is privacy-preserving and robust to data poisoning attacks. The performances obtained in both scenarios are evaluated in terms of accuracy, precision, recall, and F1-scores for healthy and sick classes. The results are compared to evaluate the cost of implementing the proposed system. The CNN model in both scenarios is trained with the same parameters for a correct comparison. Specifically, the model has been trained with 50 epochs and batch size 32 using the ‘early stopping’ approach with the patience of 5 epochs to prevent overfitting. The results obtained in the first and second scenarios and their comparison have been detailed in Sections 4.2, 4.3, and 4.4, respectively.

4.1 Datasets

For the experiments, OASIS and ADNI datasets were used. Open Access Series of Imaging Studies (OASIS) (Marcus et al., 2007) dataset is a cross-sectional RGB MRI image collection of 416 subjects aged between 18 and 96 years. One hundred of these subjects older than 60 years have been clinically diagnosed with very mild to moderate AD. The subjects include both men and women. For each subject, 3 or 4 individual T1-weighted MRI scans obtained in single scan sessions are included. Data-augmentation techniques based on image manipulation have been used to solve the dataset

imbalance. Techniques perform slight editing operations on an image, including rotations, extensions, and compressions. At the end of the data-augmentation technique, a balanced dataset of 526 RGB MRI images of healthy subjects and 526 RGB MRI images of subjects with AD has been obtained.

The Alzheimer’s Disease Neuroimaging Initiative (ADNI) dataset (Jack et al., 2008) includes 6400 cross-sectional RGB MRI images of 3200 healthy and 3200 subjects with AD. The images represent. The dataset is balanced, and then no data-augmentation technique is applied.

4.2 Results in Traditional ML Scenario

The first experiment consists of testing the CNN performance in the no-FL scenario. The datasets are divided into train and test sets using an 80 - 20 ratio. The results are reported in Table 1.

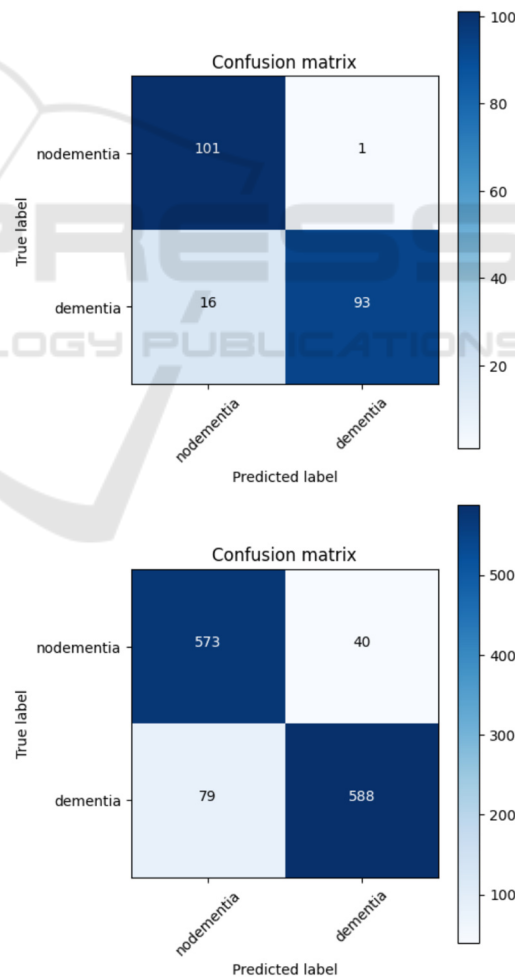


Figure 5: a) Confusion matrix of OASIS dataset. b) confusion matrix of the ADNI dataset.

Table 1: Results of CNN model in no-FL scenario.

Metrics	OASIS	ADNI
Accuracy	91.94%	90.70%
Precision	98.06%	93.47%
Recall	86.32%	87.88%
F1-score	92.94%	90.59%

The results for each healthy and AD class are reported in the confusion matrix in Figure 5. The CNN model shows the best performance in healthy subject recognition with an accuracy of healthy subject recognition of 99.02% and 93.47% for the OASIS and ADNI datasets, respectively. The accuracy in AD recognition is 85.32% and 88.16% for OASIS and ADNI datasets, respectively.

4.3 Results of the Proposed System

The second experiment tests the proposed FL with an image authentication system. Two clients that represent two medical institutions and 5 rounds of learning are used for the FL simulation. Each round represents a single iteration of global model update as discussed in Section 3.2. Each client implements the same CNN model, and the datasets are divided equally among clients. Specifically, the training set for each dataset is split 50-50 between the two clients, preserving the balance of the classes. The proposed image authentication approach is applied to each training image, and then the fingerprint image is embedded into each RGB MRI image before model training. Subsequently, the fingerprint image has been extracted and the RGB MRI image without the fingerprint is given as input to CNN. The proposed simulation is necessary to thoroughly validate the proposed system because the proposed image authentication technique inevitably reduces RGB MRI images quality. Therefore, the experiments have a dual purpose of evaluating how the image quality reduction impacts the model performance and evaluating the impact of the FL strategy. The results in terms of accuracy for each learning round are reported in Table 2.

Table 2: Accuracy results of the proposed system.

	OASIS	ADNI
Round 1	89.20%	82.06%
Round 2	89.61%	84.64%
Round 3	89.61%	85.34%
Round 4	92.00%	86.98%
Round 5	92.00%	88.50%

Table 2 shows that the proposed system improves the performance at each iteration until the optimal performance of the global model is obtained at the

fifth iteration with 92% and 88.50% accuracy for the OASIS and ADNI datasets, respectively.

4.4 Comparison of Results

The results obtained with the traditional and the proposed system in terms of accuracy are compared in Figure 6 and Figure 7 for the OASIS and ADNI datasets, respectively. Figures 6 and 7 show how the proposed system's accuracy matches the traditional system's accuracy during the 5 rounds of FL. The results of the final FL models are comparable with the results of the traditional system, with an accuracy degradation of 2.20% in the ADNI dataset and an accuracy improvement of 0.06% in the case of the OASIS dataset. Therefore, the proposed system ensures performance comparable with a traditional system, ensuring privacy and mitigating data poisoning attacks. The system is efficient on both tested datasets that are heterogeneous in data quantity, image resolution, and scanning perspective. Therefore, the system is flexible in processing and learning multiple types of information of different quantities and qualities.

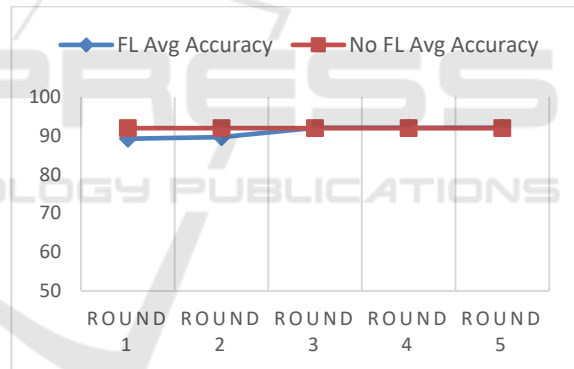


Figure 6: Comparison of results between FL and no FL approach for the OASIS dataset.

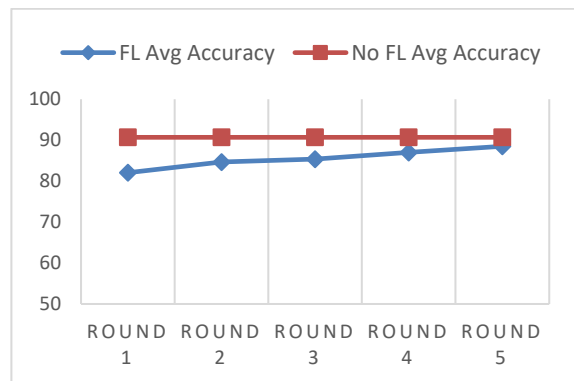


Figure 7: Comparison of results between FL and no FL approach for the ADNI dataset.

5 CONCLUSIONS

A system based on FL environment and MRI images authentication to predict AD from RGB MRI brain images has been proposed. The proposed system combines the potential of machine learning systems with protecting the privacy of sensitive data and patient information and is robust to data poisoning attacks that could cause disastrous consequences in a healthcare application. The proposed system is a solution to introduce AD recognition in a healthcare context to support physicians. The proposed system is compliance with stringent requirements of privacy and security in GDPR and other international regulations. Experiments have shown that the proposed system has a good trade-off between safety and performance. The accuracy in AD recognition is degraded by 2.20% with the ADNI dataset and it is improved by 0.06% with the OASIS dataset using the proposed system. The proposed system is tested, simulating an FL scenario with two medical institutions. In the future, the proposed system could be tested with a large number of medical institutions using a more significant number of MRI images. Moreover, multimodal AD recognition could be implemented using MRI images with different scanning perspectives and other medical information. The proposed system is privacy-preserving and prevents data poisoning attacks but there are other potential security issues in FL, such as model reversal attacks and compromise attacks on the global model that have not been considered. In the future, the security of the proposed system could be improved by implementing defense strategies against these attacks.

ACKNOWLEDGEMENTS

Francesco Castro is a PhD student enrolled in the National PhD in Artificial Intelligence, XXXVIII cycle, course on Health and life sciences, organized by Università Campus Bio-Medico di Roma.

REFERENCES

- Angelillo, M. T., Balducci, F., Impedovo, D., Pirlo, G., & Vessio, G. (2019). Attentional Pattern Classification for Automatic Dementia Detection. *IEEE Access*, 7, 57706–57716. <https://doi.org/10.1109/ACCESS.2019.2913685>
- Angelillo, M. T., Impedovo, D., Pirlo, G., & Vessio, G. (2019). Performance-Driven Handwriting Task Selection for Parkinson's Disease Classification. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11946 LNAI, 281–293. https://doi.org/10.1007/978-3-030-35166-3_20/COVER
- Bercea, C. I., Wiestler, B., Rueckert, D., & Albarqouni, S. (2022). Federated disentangled representation learning for unsupervised brain anomaly detection. *Nature Machine Intelligence* 2022 4:8, 4(8), 685–695. <https://doi.org/10.1038/s42256-022-00515-2>
- Cannarile, A., Dentamaro, V., Galantucci, S., Iannacone, A., Impedovo, D., & Pirlo, G. (2022). Comparing Deep Learning and Shallow Learning Techniques for API Calls Malware Prediction: A Study. *Applied Sciences* 2022, Vol. 12, Page 1645, 12(3), 1645. <https://doi.org/10.3390/APP12031645>
- Carrera, F., Dentamaro, V., Galantucci, S., Iannacone, A., Impedovo, D., & Pirlo, G. (2022). Combining Unsupervised Approaches for Near Real-Time Network Traffic Anomaly Detection. *Applied Sciences* 2022, Vol. 12, Page 1759, 12(3), 1759. <https://doi.org/10.3390/APP12031759>
- Castro, F., Impedovo, D., & Pirlo, G. (2023). A Medical Image Encryption Scheme for Secure Fingerprint-Based Authenticated Transmission. *Applied Sciences* 2023, Vol. 13, Page 6099, 13(10), 6099. <https://doi.org/10.3390/APP13106099>
- CHAN-HON-TONG, A. (2018). An Algorithm for Generating Invisible Data Poisoning Using Adversarial Noise That Breaks Image Classification Deep Learning. *Machine Learning and Knowledge Extraction* 2019, Vol. 1, Pages 192-204, 1(1), 192–204. <https://doi.org/10.3390/MAKE1010011>
- Cheriet, M., Dentamaro, V., Hamdan, M., Impedovo, D., & Pirlo, G. (2023). Multi-speed transformer network for neurodegenerative disease assessment and activity recognition. *Computer Methods and Programs in Biomedicine*, 230. <https://doi.org/10.1016/J.CMPB.2023.107344>
- Cicirelli, G., Impedovo, D., Dentamaro, V., Marani, R., Pirlo, G., & D’Orazio, T. R. (2022). Human Gait Analysis in Neurodegenerative Diseases: A Review. *IEEE Journal of Biomedical and Health Informatics*, 26(1), 229–242. <https://doi.org/10.1109/JBHI.2021.3092875>
- Dentamaro, V., Convertini, V. N., Galantucci, S., Giglio, P., Palmisano, T., & Pirlo, G. (2021). Ensemble consensus: An unsupervised algorithm for anomaly detection in network security data. *CEUR WORKSHOP PROCEEDINGS*, 2940, 309–318. <https://ricerca.uniba.it/handle/11586/377597>
- Dentamaro, Vincenzo, Impedovo, D., & Pirlo, G. (2018). LICIC: Less Important Components for Imbalanced Multiclass Classification. *Information* 2018, Vol. 9, Page 317, 9(12), 317. <https://doi.org/10.3390/INFO9120317>
- Dentamaro, Vincenzo, Impedovo, D., & Pirlo, G. (2021). An Analysis of Tasks and Features for Neuro-Degenerative Disease Assessment by Handwriting. *Lecture Notes in Computer Science (Including*

- Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*), 12661 LNCS, 536–545. https://doi.org/10.1007/978-3-030-68763-2_41/COVER
- Galantucci, S., Impedovo, D., & Pirlo, G. (2021). One time user key: A user-based secret sharing XOR-ed model for multiple user cryptography in distributed systems. *IEEE Access*, 9, 148521–148534. <https://doi.org/10.1109/ACCESS.2021.3124637>
- Gattulli, V., Impedovo, D., Pirlo, G., & Sarcinella, L. (2023). Human Activity Recognition for the Identification of Bullying and Cyberbullying Using Smartphone Sensors. *Electronics* 2023, Vol. 12, Page 261, 12(2), 261. <https://doi.org/10.3390/ELECTRONICS12020261>
- Gattulli, V., Impedovo, D., Pirlo, G., & Semeraro, G. (2022). Early Dementia Identification: On the Use of Random Handwriting Strokes. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 13424 LNCS, 285–300. https://doi.org/10.1007/978-3-031-19745-1_21
- Gattulli, V., Impedovo, D., Pirlo, G., & Semeraro, G. (2023). Handwriting Task-Selection based on the Analysis of Patterns in Classification Results on Alzheimer Dataset. *CEUR Workshop Proceedings*, 3521, 18–29.
- Ghosh, T., Palash, M. I. A., Yousuf, M. A., Hamid, M. A., Monowar, M. M., & Alassafi, M. O. (2023a). A Robust Distributed Deep Learning Approach to Detect Alzheimer's Disease from MRI Images. *Mathematics* 2023, Vol. 11, Page 2633, 11(12), 2633. <https://doi.org/10.3390/MATH11122633>
- Ghosh, T., Palash, M. I. A., Yousuf, M. A., Hamid, M. A., Monowar, M. M., & Alassafi, M. O. (2023b). A Robust Distributed Deep Learning Approach to Detect Alzheimer's Disease from MRI Images. *Mathematics* 2023, Vol. 11, Page 2633, 11(12), 2633. <https://doi.org/10.3390/MATH11122633>
- Han, B., Jhaveri, R. H., Wang, H., Qiao, D., & Du, J. (2023). Application of Robust Zero-Watermarking Scheme Based on Federated Learning for Securing the Healthcare Data. *IEEE Journal of Biomedical and Health Informatics*, 27(2), 804–813. <https://doi.org/10.1109/JBHI.2021.3123936>
- Impedovo, D., Pirlo, G., Sarcinella, L., Stasolla, E., & Trullo, C. A. (2012). Analysis of stability in static signatures using cosine similarity. *Proceedings - International Workshop on Frontiers in Handwriting Recognition, IWFHR*, 231–235. <https://doi.org/10.1109/ICFHR.2012.180>
- Jack, C. R., Bernstein, M. A., Fox, N. C., Thompson, P., Alexander, G., Harvey, D., Borowski, B., Britson, P. J., Whitwell, J. L., Ward, C., Dale, A. M., Felmlee, J. P., Gunter, J. L., Hill, D. L. G., Killiany, R., Schuff, N., Fox-Bosetti, S., Lin, C., Studholme, C., ... Weiner, M. W. (2008). The Alzheimer's Disease Neuroimaging Initiative (ADNI): MRI methods. *Journal of Magnetic Resonance Imaging: JMRI*, 27(4), 685–691. <https://doi.org/10.1002/JMRI.21049>
- Kaissis, G., Ziller, A., Passerat-Palmbach, J., Ryffel, T., Usynin, D., Trask, A., Lima, I., Mancuso, J., Jungmann, F., Steinborn, M. M., Saleh, A., Makowski, M., Rueckert, D., & Braren, R. (2021). End-to-end privacy preserving deep learning on multi-institutional medical imaging. *Nature Machine Intelligence* 2021 3:6, 3(6), 473–484. <https://doi.org/10.1038/s42256-021-00337-8>
- Khalil, K., Khan Mamun, M. M. R., Sherif, A., Elersy, M. S., Imam, A. A. A., Mahmoud, M., & Alsabaan, M. (2023). A Federated Learning Model Based on Hardware Acceleration for the Early Detection of Alzheimer's Disease. *Sensors* 2023, Vol. 23, Page 8272, 23(19), 8272. <https://doi.org/10.3390/S23198272>
- Li, Q., He, B., & Song, D. (2021). Model-Contrastive Federated Learning. *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 10708–10717. <https://doi.org/10.1109/CVPR46437.2021.01057>
- Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y., Liu, X., & He, B. (2021). A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection. *IEEE Transactions on Knowledge and Data Engineering*. <https://doi.org/10.1109/TKDE.2021.3124599>
- Marcus, D. S., Wang, T. H., Parker, J., Csernansky, J. G., Morris, J. C., & Buckner, R. L. (2007). Open Access Series of Imaging Studies (OASIS): Cross-sectional MRI Data in Young, Middle Aged, Nondemented, and Demented Older Adults. *Journal of Cognitive Neuroscience*, 19(9), 1498–1507. <https://doi.org/10.1162/JOCN.2007.19.9.1498>
- Mirzaei, G., & Adeli, H. (2022). Machine learning techniques for diagnosis of alzheimer disease, mild cognitive disorder, and other types of dementia. *Biomedical Signal Processing and Control*, 72, 103293. <https://doi.org/10.1016/J.BSPC.2021.103293>
- Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. *Future Generation Computer Systems*, 115, 619–640. <https://doi.org/10.1016/J.FUTURE.2020.10.007>
- Narmadha, K., & Varalakshmi, P. (2022). Federated Learning in Healthcare: A Privacy Preserving Approach. *Studies in Health Technology and Informatics*, 294, 194–198. <https://doi.org/10.3233/SHTI220436>
- Nguyen, T. V., Dakka, M. A., Diakiw, S. M., VerMilyea, M. D., Perugini, M., Hall, J. M. M., & Perugini, D. (2022). A novel decentralized federated learning approach to train on globally distributed, poor quality, and protected private medical data. *Scientific Reports* 2022 12:1, 12(1), 1–12. <https://doi.org/10.1038/s41598-022-12833-x>
- Salehi, A. W., Baglat, P., Sharma, B. B., Gupta, G., & Upadhyaya, A. (2020). A CNN Model: Earlier Diagnosis and Classification of Alzheimer Disease using MRI. *Proceedings - International Conference on Smart Electronics and Communication, ICOSEC 2020*, 156–161. <https://doi.org/10.1109/ICOSEC49089.2020.9215402>

- Sivan, R., & Zukarnain, Z. A. (2021). Security and Privacy in Cloud-Based E-Health System. *Symmetry* 2021, Vol. 13, Page 742, 13(5), 742. <https://doi.org/10.3390/SYM13050742>
- Suresha, H. S., & Parthasarathy, S. S. (2020). Alzheimer Disease Detection Based on Deep Neural Network with Rectified Adam Optimization Technique using MRI Analysis. *Proceedings of 2020 3rd International Conference on Advances in Electronics, Computers and Communications, ICAECC 2020*. <https://doi.org/10.1109/ICAIECC50550.2020.9339504>
- Wang, S. H., Phillips, P., Sui, Y., Liu, B., Yang, M., & Cheng, H. (2018). Classification of Alzheimer's Disease Based on Eight-Layer Convolutional Neural Network with Leaky Rectified Linear Unit and Max Pooling. *Journal of Medical Systems*, 42(5), 1–11. <https://doi.org/10.1007/S10916-018-0932-7/FIGURES/11>
- Wen, J., Thibeau-Sutre, E., Diaz-Melo, M., Samper-González, J., Routier, A., Bottani, S., Dormont, D., Durrleman, S., Burgos, N., & Colliot, O. (2020). Convolutional neural networks for classification of Alzheimer's disease: Overview and reproducible evaluation. *Medical Image Analysis*, 63, 101694. <https://doi.org/10.1016/J.MEDIA.2020.101694>
- Zhang, L., Xu, J., Vijayakumar, P., Sharma, P. K., & Ghosh, U. (2023). Homomorphic Encryption-Based Privacy-Preserving Federated Learning in IoT-Enabled Healthcare System. *IEEE Transactions on Network Science and Engineering*, 10(5), 2864–2880. <https://doi.org/10.1109/TNSE.2022.3185327>
- Zhao, L., & Huang, J. (2023). A distribution information sharing federated learning approach for medical image data. *Complex and Intelligent Systems*, 9(5), 5625–5636. <https://doi.org/10.1007/S40747-023-01035-1/FIGURES/11>