PRIVACY-PRESERVING FEDERATED DEEP-EQUILIBRIUM LEARNING FOR MEDICAL IMAGE CLASSIFICATION

Alexandros Gkillas[a], *Dimitris Ampeliotis*[b], *Kostas Berberidis*[a]

[a]Dept. of Computer Engineering & Informatics, University of Patras, Greece

[b]Dept. of Digital Media and Communication, Ionian University, Greece

ABSTRACT

In this work, we study the problem of skin cancer diagnosis from images by employing a network of collaborating institutions (e.g, hospitals) that cooperate under the emerging federated learning protocol. In such a scenario, the problems of not exposing sensitive patient information as well as the heterogeneity of the participating devices are of paramount importance. To this end, we propose the use of deep equilibrium models, in place of some other "traditional" deep neural network model, that offer a natural means of dealing with devices that have different computational resources. Furthermore, to prevent the leakage of sensitive information, the models exchanged in the proposed approach are homomorpically encrypted. Numerical results indicate that the proposed approach offers the same accuracy as compared to the state-of-the-art federated learning case that "traditional" deep-learning models, but with three significant advantages: (a) increased privacy, (b) support of heterogeneous devices, and (c) significantly reduced communication requirements.

Index Terms— deep-equilibrium models, federated learning, medical imaging, homomorphic encryption

1. INTRODUCTION

The groundbreaking success of machine learning approaches has offered automated classification systems with a close-to-human performance, especially in image recognition applications. In the medical domain, computer-aided-diagnosis (CAD) systems based on deep-learning could be an invaluable tool for physicians. However, such developments are hindered by the fact that medical data contain sensitive information as well as due to General Data Protection Regulation restrictions. In particular, such concerns impose practical limitations to the collection of large medical data records, which are required for generating accurate CAD systems. Federated learning (FL) has emerged as a promising approach for privacy-preserving deep learning by distributing both data collection and model training to a number of collaborating agents. This method is particularly suited to data sensitive applications, such as in medical image classification [1]. This research identifies and addresses two primary concerns associated with the application of federated learning in the field of medical information processing [2]. The first issue pertains to privacy concerns. Although the FL concept can provide privacy protection by allowing users to keep their data at local sites during the training, it has been proven that the model weights might still contain sensitive user information such as data features that can be reconstructed by a "curious" global server [3]. The second issue involves the computational and network complexities of applying FL across various environments. Diverse hardware specifications and network conditions across different medical facilities can significantly affect the performance and implementation of FL algorithms. Such a complex, heterogeneous environment gives rise to the Internet-of-Medical-Things (IoMT) [3].

Existing literature, such as [4] primarily focuses on privacy in federated learning without considering the computational heterogeneity. Conversely, studies like [5–7], and [8] address device heterogeneity but can neglect privacy concerns and suffer performance losses, which are critical issues in the IoMT domain. For instance, in [5] only a subset of collaborating devices is selected, potentially overlooking valuable data from less powerful institutions. In [6] the authors employ a global model that can fit to the minimum capabilities of all clients, which may compromise the overall model performance. Another direction relies on deploying different models across clients adapted to their computational resources, as in study [8]. However, the implementation of such approaches can be a challenging task due to the complex aggregation rules required.

Contribution: Different from the above mentioned works, our research takes a novel approach by addressing both privacy and computational heterogeneity in healthcare federated learning (FL), while maintaining high system performance without necessitating overly complex solutions. To enhance privacy, this study considers the use of Homomorphic Encryption (HE), [9]) and combines it with federated deep equilibrium learning [10] for the first time. This approach aims to secure private local information without compromising the collective learning processes. Addressing the second challenge, unlike the existing literature, in this study, we examine FL under a different perspective, focusing on the structure and properties of the model employed by the collaborating institutions. To be more precise, rather than employing a conventional deep learning network, we utilize the Deep Equilibrium (DEQ) models [11]. We argue that these models are characterized by unique properties providing solutions to open-problems in IoMT FL, including the communication burden, as well as the computational heterogeneity of the local devices. Our study stands out by offering a methodology applicable across all federated learning (FL) algorithms, focusing on the properties of deep learning models used in FL. This approach allows state-of-the-art algorithms such as [7] , aimed at simplifying FL complexity, to be enhanced through the deployment of deep equilibrium models, making it a versatile solution for improving FL systems.

2. PRELIMINARIES - DEQ MODELS

The DEQ model relies on the concept of a fixed point iteration where the neural network, instead of having distinct parameters / weights for each layer, uses the same (weight-tied) parameters for all layers [11]. This is described by

$$z^{(k+1)} = \sigma(Wz^{(k)} + Ux + b) \tag{1}$$

where, x is the input, $\boldsymbol{U}$ represents the input-injection weights, $z^{(k)}$ denotes the hidden unit activations at iteration k, $\boldsymbol{W}$ represents the weight matrix, b is the bias term, and σ stands for the activation function. The output of the DEQ model is given as the fixed point z^* such that:

$$z^* = \sigma(Wz^* + Ux + b) = f_\theta(z^\star, x) \tag{2}$$

where $f_\theta(z, x) = \sigma(\mathbf{W}z + \mathbf{U}x + b)$ is the transformation of the DEQ model. In other words, the output of a DEQ model is the fixed point $z^\star$ where any further application of the transformation $f_\theta(\cdot, x)$ would not alter its value.

3. PROPOSED METHOD

3.1. Federated DEQ Learning for Medical Imaging

Consider that a consortium of N institutions, such as hospitals, is engaged in a joint effort to develop a deep equilibrium model for diagnosing skin cancer from medical images. Each institution n, where $n \in \mathcal{N} = \{1, 2, \ldots, N\}$, possesses a training dataset $\mathcal{D}_n = (x_{i,n}, y_{i,n})_{i=1}^{|D_n|}$, with $x_{i,n}$ representing patient images (input), $y_{i,n}$ signifying the associated skin cancer class (output). The objective of each institution n is to train an individual DEQ model with parameters θ_n by minimizing a local loss function $\mathcal{L}_n(\cdot)$. This process involves repeatedly solving several fixed-point problems to compute the outputs of the DEQ model for the given data. The local objective for an institution n is defined as

$$g_n(\theta_n; \mathcal{D}_n) = \frac{1}{|\mathcal{D}_n|} \sum_{i=1}^{|\mathcal{D}_n|} \mathcal{L}_n(z^\star_{i,n}, y_{i,n}) \ , \tag{3}$$

where $z^*_{i,n}$ represents the fixed-point solution satisfying $z^*_{i,n} = f_{\theta_n}(z^*_{i,n}, x_{i,n})$. This fixed-point solution corresponds to the output of the DEQ model when patient image $x_{i,n}$ is given as input. Based on the Federated DEQ learning (FL-DEQ) method, the clients aim to collaborate without exchanging any private data, thus deriving a global DEQ model, say θ_g. The overall objective of the FL-DEQ scheme is to minimize the aggregation of the local objectives, given by

$$G(\theta_g) = \sum_{n=1}^{N} w_n g_n(\theta_n; \mathcal{D}_n) \ , \tag{4}$$

where w_n denote some weight coefficients that balance the impact of each local objective function.

3.2. Institution side-local update: forward and backward pass

In the DEQ model framework, the transformation $f_\theta(\cdot, x)$ in (2) is iteratively applied until equilibrium is reached. On the client side, this presents two main computational challenges. Firstly, during the **forward pass**, it is essential to efficiently compute the equilibrium point z^* for an input $x_{i,n}$ using the transformation $f_{\theta_n}(\cdot, x_{i,n})$. Secondly, in the **backward pass**, the clients (e.g., hospitals) need to update the weights of their local DEQ models towards minimizing a local loss function.

Focusing on the **forward pass**, the Anderson acceleration technique is employed [11], which significantly speeds up the convergence towards the fixed point $z^\star$. Concerning the **backward pass**, the client updates its DEQ model by minimizing some loss function. Instead of backpropagating through numerous fixed-point iterations, the implicit function theorem is employed to simplify the gradient computation process [11]. This allows for an efficient update of the model's weights during training.

3.3. Properties of the DEQ models in FL: Heterogeneous computational capabilities

DEQ models have the advantage of offering a natural solution to the problem of **heterogeneous** devices in federated learning. In particular, the architecture of the DEQ model can adapt dynamically depending on the computational capabilities of the clients devices. This is accomplished by varying the number of fixed-point iterations performed on the clients, according to their resources. Therefore, client devices with limited computational resources may use a smaller number of fixed point iterations as compared to other devices with more powerful hardware. This dynamic adaptation of DEQ models to varying computational capabilities of edge devices allows them to participate in the learning process using a smaller number of fixed point iterations, thus facilitating the deployment of federated learning in heterogeneous environments. Furthermore, DEQ models require fewer parameters for transmission as compared to traditional deep networks, thus leading to reduced communication costs and computational overhead.

3.4. Introducing Privacy on the FL-DEQ

In this work, considering the importance of privacy in medical imaging applications, we incorporate homomorphic encryption [9] into Federated Deep Equilibrium Learning. Our goal is to showcase the straightforward integration of HE, reinforcing the security of the FL-DEQ without compromising model efficacy. HE is critical for privacy in FL-DEQ, enabling computation on encrypted weights of the local DEQ models to protect client confidentiality using two cryptographic keys throughout the learning process: (i) the **public key**: each client uses this key to encrypt its local DEQ model ensuring that the server has access only on the encrypted local models and (ii) the **private key**: this key remains solely with the clients and it is used to decrypt the encrypted weights of the DEQ models. The process flows as follows:

- **Local Training and Encryption:** Clients individually train DEQ models on their data and subsequently encrypt the model parameters using the public key. The encrypted models are sent to a central server.
- **Encrypted Domain Aggregation:** The server performs computations such as averaging on the encrypted models without decrypting them. The homomorphic property of HE ensures that the resulting encrypted model, when decrypted, aligns with the outcomes as if the operations had been performed in the unencrypted domain.
- **Decryption and Updating:** The clients decrypt the aggregated global model with their private keys and this model is used to initialize the next local update iteration.

The HE was implemented using the Tenseal library [1].

3.5. Server-side - Encrypted Domain Aggregation

On the server-side, to accommodate the heterogeneity in the computational capabilities of each client and the fact that the clients utilize a different number of fixed-point iterations, we propose a weighted averaging fusion rule that takes into account the number of iterations that each client performs. Specifically, since the models coming from clients that perform more iterations are expected to be more accurate, these models are given greater weights. The server, merges the encrypted models using the fusion rule without decrypting them. In more detail, at each communication round t, the server computes the encrypted global model using the rule:

$$\text{Enc}(\theta_g^{(t)}) = \frac{1}{\sum_{n=1}^{N} u_n} \sum_{n=1}^{N} u_n \cdot \text{Enc}(\theta_n^{(t)}) \,, \tag{5}$$

where $\text{Enc}(\theta_g^{(t)})$ is the encrypted global model, $\text{Enc}(\theta_n^{(t)})$ is the encrypted DEQ model sent by client n, and u_n is the number of fixed-point iterations executed by client n.

4. EXPERIMENTAL PART

4.1. Implementation details

Dataset and settings: We use the HAM10000 dataset [12], a large set of 10,015 dermatoscopic images called ”Human Against Machine with 10,000 training images”. For the FL experiments, we consider non-IID data case where the label ratios follow the Dirichlet distribution, similar to study [13] **The choice of DEQ model (transformation $f_\theta(.)$):** Considering that the ResNet network achieves state-of-the-art performance on the examined dataset [14], we adopted a DEQ model that integrates a transformation derived from ResNet. Thus, the transformation f_θ in the DEQ model is a residual block

$$f_\theta(z, x) = \mathcal{B}(\sigma(z + \mathcal{B}(x + \mathbf{W}_2 * \mathcal{B}(\sigma(\mathbf{W}_1 * z))))))$$

where $\mathcal{B}$ is the Group normalization and σ denotes the ReLU. Note that the DEQ model may comprise of additional residual blocks to achieve a balance between accuracy and number of parameters. **Parameters:** Each FL method utilized 200 communication rounds between the server and the clients. Concerning the local training, we employed 1 epoch with batch size equal to 128. Also, we employ 15 fixed point iterations.

4.2. Results: Computational Efficiency and Privacy

As illustrated in Table 1, the FL-DEQ approach is particularly effective in the context of smart IoMT, taking into account the varying computational resources across institutions and the critical importance of data confidentiality. FL-DEQ not only delivers accuracy on par with current state-of-the-art FL methods in medical imaging, but it also excels in reducing model complexity and achieving significant compression rates, more than 97.27%. Moreover, the integration of HE enhances data privacy without undermining accuracy, making FL-DEQ an ideal solution for healthcare where both data security and high model efficiency are essential.

4.3. Results: Heterogeneous Devices

Table 2 highlights the resilience and adaptability of the Federated Deep Equilibrium (FL-DEQ) approach, especially in scenarios characterized by varying computational resources, as often encountered in IoMT systems. In our study, we modeled a scenario where 40% of the clients, due to limited in computational power, perform only 3 fixed point iterations during local updates, while more powerful clients complete 15 iterations. This setup was evaluated in two contexts: a homogeneous scenario where all devices uniformly conducted 15 iterations, and a heterogeneous scenario with varying iteration counts based on device capability. The results demonstrate that FL-DEQ is able effectively manages these disparities in computational resources, achieving consistent performance in both considered scenarios. This robustness is crucial

[1] https://github.com/OpenMined/TenSEAL

Table 1: Comparison of FL-DEQ using DEQ models with one (FL-DEQ-1) and three (FL-DEQ-3) residual blocks and with and without Homomorphic Encryption (HE) against standard FL methods employing the ResNet-18 model (10 clients).

Dataset		FedAvg [15]	FedProx [16]	SplitFed [14]	FedGKT [17]	**FL-DEQ-1-Block** with HE	**FL-DEQ-3-Blocks** with HE	**FL-DEQ-1-Block** without HE	**FL-DEQ-3-Blocks** without HE
HAM10000	Accuracy	77.5%	78.05%	79.2%	74.11%	77.3%	79.1%	77.3%	79.1%
	No. Param (Milions)	11M	11M	11M	11M	0.06M	0.2M	0.06M	0.2M
	Compression Rate	-	-	-	-	99.45%	97.27%	99.45%	97.27%

Table 2: The FL-DEQ in a heterogeneous scenario is resilient to varying computational resources of clients.

	Homogeneous Scenario	Heterogeneous Scenario	No. Param (Milions)
FL-DEQ-1-Block	77.3%	76.4%	0.06M
FL-DEQ-3-Block	79.1%	78.6%	0.2M

in the healthcare sector, where institutions may have significantly different technological capabilities, yet require consistent performance in handling sensitive patient data.

5. CONCLUSIONS

A novel FL-DEQ method is presented combining deep equilibrium models with Homomorphic Encryption to tackle challenges in healthcare federated learning. This method adapts to different computational capacities and secures model exchanges, showing promising results in diagnostic accuracy, data privacy, and operation in varied computational settings. Future work will focus on improving privacy without needing uniform encryption keys and exploring the effect of other encryption methods like differential privacy on performance.

6. REFERENCES

[1] Dianwen Ng, Xiang Lan, Melissa Min-Szu Yao, Wing P Chan, and Mengling Feng, "Federated learning: a collaborative effort to achieve better medical imaging models for individual sites that have small labelled datasets," *Quantitative Imaging in Medicine and Surgery*, vol. 11, no. 2, pp. 852, 2021.

[2] Erfan Darzidehkalani, Mohammad Ghasemi-rad, and P.M.A. van Ooijen, "Federated learning in medical imaging: Part ii: Methods, challenges, and considerations," *J. of the American College of Radiology*, vol. 19, no. 8, pp. 975–982, 2022.

[3] Dinh C. Nguyen, Quoc-Viet Pham, Pubudu N. Pathirana, and et al, "Federated learning for smart healthcare: A survey," *ACM Comput. Surv.*, vol. 55, no. 3, feb 2022.

[4] Mohammed Adnan, Shivam Kalra, Jesse C Cresswell, Graham W Taylor, and Hamid R Tizhoosh, "Federated learning and differential privacy for medical image analysis," *Scientific reports*, vol. 12, no. 1, pp. 1953, 2022.

[5] Keith Bonawitz and et. al, "Towards federated learning at scale: System design," in *Machine Learning and Systems*, 2019, vol. 1, pp. 374–388.

[6] Chenhao Xu, Youyang Qu, Yong Xiang, and Longxiang Gao, "Asynchronous federated learning on heterogeneous devices: A survey," *CoRR*, vol. abs/2109.04269, 2021.

[7] Xidong Wu, Feihu Huang, Zhengmian Hu, and Heng Huang, "Faster adaptive federated learning," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 37, no. 9, pp. 10379–10387, Jun. 2023.

[8] Jie Zhang, Song Guo, Xiaosong Ma, Haozhao Wang, Wenchao Xu, and Feijie Wu, "Parameterized knowledge transfer for personalized federated learning," in *Advances in Neural Information Processing Systems*, 2021.

[9] Abbas Acar, Hidayet Aksu, A Selcuk Uluagac, and Mauro Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Computing Surveys (Csur)*, vol. 51, no. 4, pp. 1–35, 2018.

[10] Alexandros Gkillas, Dimitris Ampeliotis, and Kostas Berberidis, "Deep equilibrium models meet federated learning," in *2023 EUSIPCO*, 2023, pp. 1873–1877.

[11] Shaojie Bai, J Zico Kolter, and Vladlen Koltun, "Deep Equilibrium Models," in *Advances in Neural Information Processing Systems*. 2019, vol. 32, Curran Associates, Inc.

[12] Philipp Tschandl, Cliff Rosendahl, and Harald Kittler, "The ham10000 dataset, a large collection of multi-source dermatoscopic images of common pigmented skin lesions," *Scientific data*, vol. 5, no. 1, pp. 1–9, 2018.

[13] Hong-You Chen and Wei-Lun Chao, "On bridging generic and personalized federated learning for image classification," in *Int. Conf. on Learning Representations*, 2022.

[14] Chandra Thapa, Pathum Chamikara Mahawaga Arachchige, Seyit Camtepe, and Lichao Sun, "Splitfed: When federated learning meets split learning," in *e AAAI Conf. on Artif. Intelligence*, 2022, vol. 36, pp. 8485–8493.

[15] H. Brendan McMahan, Eider Moore, Daniel Ramage, and Blaise Agüera y Arcas, "Federated learning of deep networks using model averaging," *CoRR*, vol. abs/1602.05629, 2016.

[16] Tian Li, Anit Kumar Sahu, Manzil Zaheer, Maziar Sanjabi, Ameet Talwalkar, and Virginia Smith, "Federated optimization in heterogeneous networks," *Machine learning and systems*, vol. 2, pp. 429–450, 2020.

[17] Chaoyang He, Murali Annavaram, and Salman Avestimehr, "Group knowledge transfer: Federated learning of large cnns at the edge," *Advances in Neural Information Processing Systems*, vol. 33, pp. 14068–14080, 2020.