Preserving Medical Data Privacy with Federated Learning

Adria Binte Habib
School of Data and Sciences
Brac University, Dhaka, Bangladesh
adria.habib@bracu.ac.bd

Abdullah Umar Nasib
School of Data and Sciences
Brac University, Dhaka, Bangladesh
abdullah.umar.nasib@g.bracu.ac.bd

Md. Sabbir Hossain
School of Data and Sciences
Brac University, Dhaka, Bangladesh
md.sabbir.hossain@g.bracu.ac.bd

Annajiat Alim Rasel
School of Data and Sciences
Brac University, Dhaka, Bangladesh
annajiat@gmail.com

***Abstract*—Many jurisdictions consider privacy to be a fundamental human right, and data protection laws exist to protect that right. Data privacy is also important because individuals must trust that their personal data will be handled with care in order to engage online. However, nowadays, data privacy is getting hampered in different ways, specially in medical sectors. To address this issue, we brought a federated learning based model which will deliver more accurate result while maintaining the data privacy of other hospital's data.**

***Index Terms*—Federated Learning, Medical Data, Machine Learning, Data Mining.**

I. Introduction

Modern technologies introduced new technologies in our medical system that involves a significant amount of medical data in daily basis. The threads of data privacy violation is also tremendous along with the advancement of technology. This issue requires an special attention to deal with the privacy thread where Federated Learning comes into play. Like most other machine learning algorithms, Federated Learning is data hungry and that makes it a hot cake to work on protecting medical data.

Due to the complexity of the healthcare system and operations, healthcare data are frequently fragmented. For instance, various hospitals could only be allowed to view the clinical records of the patients who belong to their particular patient groups. These documents include highly private health information (PHI) about specific people. Strict laws, such as the Health Insurance Portability and Accountability Act (HIPAA), have been devised to regulate the process of accessing and analyzing such data [1]. Modern data mining and machine learning (ML) technologies, such deep learning, which normally needs a vast quantity of training data, are faced with a significant difficulty as a result.

Federated learning is a paradigm that has gained prominence recently due to its enormous potential for learning from sensitive data that is dispersed. It enables training a shared global model using a central server while maintaining the data in local institutions where they originate, as opposed to aggregating data from several sources all at once or depending on the conventional discovery then replication method.

Thus, a successful FL implementation could have a significant impact on the ability to practice precision medicine on a large scale, resulting in models that produce objective judgments, accurately reflect the physiology of an individual, are sensitive to rare diseases, and respect governance and privacy concerns. FL still needs careful technical analysis to make sure that the algorithm is working as efficiently as possible without endangering patient privacy or safety. Nonetheless, it has the ability to get around the drawbacks of strategies that call for a single pool of centralized data.

The data receives additional protection because federated learning makes it feasible to jointly train a model with data from several users without letting any raw data leave their devices. This is the actual aim of our study. To obtain more accurate medical data while maintaining top-notch data privacy, we will train the medical photos from various clients.

II. Related Works

A noticeable amount of researches has already been done and published on Federated Learning which are also freely available.

In a related work, Nicola Rieke and his colleagues demonstrated their consensus view targeting of providing context and detail for the community regarding the advantages and impacts of FL for medical applications besides highlighting key considerations and challenges of implementing FL for digital health [2]. They highly believed that Federated Learning has the potentials to minimise the obstacles of approaches that require a single pool of centralised data.

Jei Xu et. al. has done their research with the goal of providing a review for federated learning technologies, particularly within the biomedical space [3]. Additionally, they summarized the general solutions to the statistical challenges, system challenges, and privacy issues in federated learning, and point out the implications and potentials in healthcare.

In an extended survey, Kaiyue et al. has given a brief review of the state-of-the-art federated learning techniques and briefly discussed the improvement of federated learning [4]. The authors also discussed several open issues and existing solutions in federated learning along with pointing out the future research directions of federated learning.

Wei Yang Bryan Lim et. al. leveraged on the dynamic contract design to consider a two-period incentive mechanism that satisfies the inter temporal incentive compatibility (IIC), such that the self-revealing mechanism of the contract holds across both periods [5]. The performance evaluation showed that their contract design satisfies the IIC constraints and derives greater profits than that of the uniform pricing scheme, thus validating its effectiveness in mitigating the adverse impacts of information asymmetry.

In another research, Adnan Q. et. al. utilized an emerging concept of clustered federated learning (CFL) and proposed a CFL-based collaborative learning framework for an automatic multi-modal COVID-19 diagnosis [6]. Their approach is well suited to the task of COVID-19 diagnosis as visual data (i.e., CT scans, X-rays, and ultrasound) was collected at different centers and could be used to build a joint/shared ML model in a cloud-edge infrastructure being able to diagnose COVID-19 in both X-ray and Ultrasound images (without the requirement of sharing data with a cloud or a central entity).

III. Proposed Workflow

The proposed model consists of two main sub sections. The first one is to classification of data and the second one is to detection which are shown in Figure 1 and Figure 2 respectively.

The architecture diagram i.e Fig 1. explains how exactly the solution works at the system level. The steps to detect the most effective DL model for RBC abnormality classification are displayed here.

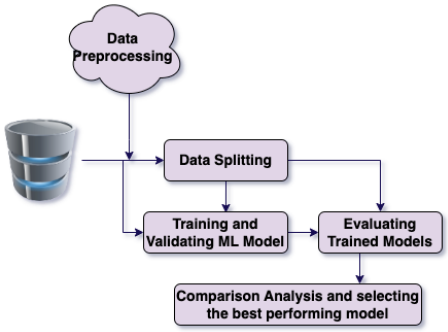

Fig. 1. Proposed Workflow of Classification of Data

In data preprocessing stage, firstly we have normalized the RBC images with Principal Component Analysis which is also known as PCA and modified them to a resolution of 128x128 pixels where it becomes more workable.

Secondly, we have split our available data in a ratio of 1:7:2 where 10% was utilized for the model's validation process where as 70% of the image was picked randomly for the purpose of training the models. The remaining 20% data was used for validation task. Finally, in our research, we have trained and made comparisons between the three DL models (VGG19, ResNet50, and Inception v3).

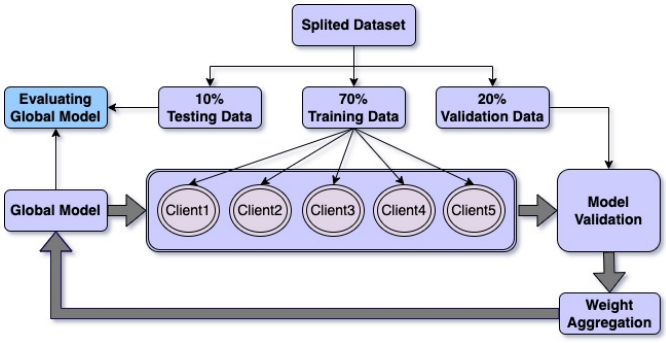

Fig. 2. Detailed Proposed Model

The experiment starts with the use of the global model named the VGG19, ResNet50, and Inception v3. Next, five clones of this global model is made to be sent to 5 separate clients. These clients, instead of working centrally, are decentralized and train the cloned models separately on their own separate data sets. After they are done running their models, the weights found from the training sessions are passed up to the central global model. After this, the 5 separate readings are merged and averaged to find a single value. After this, the global model is tested likewise.

IV. Input Dataset and Reprocessing

A. Data Collection and Data Analysis

We used a dataset that is a skin cancer dataset for our research. This dataset [7] was created by The International Skin Imaging Collaboration and has 2357 photos of both malignant and benign oncological illnesses. (ISIC). Except for melanomas and moles, whose photos have a minor predominance, all images were sorted according to the categorization determined with ISIC, and all subgroups were divided into the same number of images. The following illnesses are included in the data set: Basal cell carcinoma, dermatofibroma, melanoma, nevus, pigmented benign keratoses, seborrheic keratoses, squamous cell carcinoma, and vascular lesions are among the skin conditions that can cause keratoses.

B. Data Preprocessing

As we have seen in the previous section, there are 9 types of skin cancer information in the dataset. Since we have worked with 5 client-server systems, we distributed each type of cancer information to 5 clients. Each client got an equal number of information for all types of skin cancer. Since the dataset was not evenly distributed in the earlier phase, we did not take the remaining information after even distribution. We considered the remaining information as outliers and cut off that information.

V. Machine Learning Module

A. Algorithms

References

[1] L. O. Gostin, "National health information privacy: regulations under the health insurance portability and accountability act." [Online]. Available: 10.1001/jama.285.23.3015

[2] K. Clarkson and M. Reza, "Was that sarcasm? -a survey of machine learning models for classifying sarcastic comments on reddit using word embeddings," 12 2018.

[3] G. C. S. P. W. J. B. F. W. Jie Xu, Benjamin S, "Federated learning for healthcare informatics," *Journal of Healthcare Informatics Research (2021)*, pp. 1–19, 11 2020. [Online]. Available: https://doi.org/10.1007/s41666-020-00082-4

[4] C. Z. S. Y. Kaiyue ZHANG, Xuan SONG, "Challenges and future directions of secure federated learning: a survey," *PeerJ. Computer science*, vol. 12, 2021. [Online]. Available: https://doi.org/10.1007/s11704-021-0598-z

[5] Z. X. D. N. C. L. C. M. M. G. Wei Yang Bryan Lim, Sahil Garg, "Dynamic contract design for federated learning in smart healthcare applications," *IEEE Internet of Things Journal*, vol. 8, pp. 16 853–16 862, 10 2020. [Online]. Available: 10.1109/JIOT.2020.3033806

[6] M. A. A. A. A.-F. J. Q. Adnan Qayyum, Kashif Ahmad, "Collaborative federated learning for healthcare: Multi-modal covid-19 diagnosis at the edge," *IEEE Open Journal of Computer Society*, vol. 3, pp. 172–184, 09 2022. [Online]. Available: 10.1109/OJCS.2022.3206407

[7] A. Katanskiy, "Skin cancer isic," Aug 2019. [Online]. Available: https://www.kaggle.com/datasets/nodoubttome/skin-cancer9-classesisic