Prescription Image Based Federated Learning for Healthcare

1st Mirza Ahmad Shayer
Department of Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
mirza.ahmad.shayer@g.bracu.ac.bd

2nd Fahmida Ahmed Hridy
Department of Computer Science
BRAC University
Dhaka, Bangladesh
fahmida.ahmed@g.bracu.ac.bd

3rd Sushana Islam Mim
Department of Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
sushana.islam.mim@g.bracu.ac.bd

4th Annajiat Alim Rasel
Department of Computer Science and Engineering, Lecturer
BRAC University
Dhaka, Bangladesh
annajiat@bracu.ac.bd

5th MD Sabbir Hossain
Department of Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
sabbir.hossain@bracu.ac.bd

6th MD Farhadul Islam
Department of Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
farhadul.islam@g.bracu.ac.bd

***Abstract*—In the modern world, Machine Learning (ML) has become very popular at the forefront of many advancements in technology. It is used in many industries for solving multitudes of various problems. In recent years, a popular ML trend has become the industry standard - Federated Learning (FL). Nowadays different versions of federated learning are used in many industries. We will discuss how the different types of FL are used in the healthcare industry. We will also discuss some popular FL technologies in the healthcare industry. We will consider the pros and cons of using FL in this industry and some of the obstacles. We will also shed light on our new idea of using federated learning on prescription images and will discuss in detail a prescription image-based federated learning model for healthcare. We talk about the system model, the steps in detail, and aggregation pseudocode. We also discuss some issues with our model idea and provide solutions. Lastly, we reach a conclusion and discuss some future work. We believe FL will bring forth a data revolution in the healthcare industry.**

***Index Terms*—Machine Learning (ML), Federated Learning (FL), healthcare industry, obstacles, solutions, prescription image-based federated learning**

I. Introduction

Before the popularity of federated learning exploded, other means of obtaining datasets and measurements were utilized. However, those were very inefficient and would also often lead to errors and data mismanagement. With federated learning now becoming the norm in many industries, the healthcare industry is no exception. Due to federated learning's high capabilities in data manipulation, security and augmentation, medical researchers can almost solve any problems related to medical data or imaging analysis. Although this is not without its fair share of challenges revolving around multiple issues. According to Rieke et al., for building accurate and robust statistical models, data-driven machine learning shows a promising future. Here medical data is collected from healthcare systems in large quantities [1]. As per Rifai et al., Federated Learning and blockchain are two technologies that can handle the management of medical data as it comes from many different systems and is often distributed [2]. Although federated learning can help in the management of distributed medical data, the ethical dilemma still persists. In obtaining datasets, medical data is the hardest to come by. As per the policies and regulations of many institutes and laws involved, it is rather difficult to get medical datasets. As per Rieke et al., ML cannot access the full medical dataset due to privacy issues [1]. Rifai et al. say that medical records hold patients' personal information which can cause prejudice if it leaks out. Researchers face these ethical challenges when they handle medical data [2]. To tackle the issues of privacy and data security federated learning was used. It ensured that even if the data was used, it would be so in a secure and safe manner. Federated learning also splits workloads among many machines so processing can be done in a distributed manner very quickly. According to Yang et al, today AI faces two monumental challenges - one is that large datasets often exist as isolated islands and two is the issue of data security and privacy [3]. It is important to talk about the uses of Federated Learning in healthcare as it will bring about new ways to save lives, increase efficiency in disease treatment and reduce errors in medical research. We will talk about federated learning in the healthcare industry. We will discuss the popular FL approaches used in the healthcare industry. We will also speak of some of the advantages and disadvantages of this approach. We will shed light on some of the other challenges, ethical dilemmas, device-related issues, and limitations of using FL. Lastly, we will provide some solutions to some issues regarding FL and how to solve them or at least reduce their potency.

II. Literature Review

Federated Learning is a concept that was proposed by Google. Since many datasets and data are distributed across multiple systems, they proposed the idea of building ML models based on the distributed system without the risk of data leaking out. The system works similarly to a distributed computing system but with more complex processes that increase its efficiency, security and output. Yang et al., also says that this is very similar to privacy-preserving machine learning. On-device federated learning is the main focus and mobile user interactions are present. Communication costs in large distributions, unbalanced data spread, and device reliability is the main causes of optimization deficiencies. Also, data is partitioned using the device and personal IDs so it appears in the database in a horizontal fashion [3]. Federated Learning supersedes conventional methods, whereby all users can simultaneously train the data on multiple machines without exposing each user's private data. The real issue with federated learning is the privacy of the user's or collaborator's data. According to Treleaven, the three main issues with Federated Learning are - a) the compromise of distributed and isolated datasets by the data, b) the requirement of models to be trained across the independent datasets by the analytics, c) privacy and sovereignty legislation, increases the difficulty of analyzing, sharing and collecting data. Despite all this Federated Learning is a pivotal technology for future data ecosystems [4]. As per Alawadi, for better management of health, there is a need for privacy preservation of patient data and secure monitoring of individuals. Remote health monitoring is becoming a popular trend. Although, continuous and accurate monitoring of health status will require expert validation in active learning [5]. Malicious users may be able to produce false outputs to manipulate the DL model because FL is built on a large number of participants (particularly cross-device FL). There are privacy-preserving solutions that can be used to improve FL's privacy by leveraging safe multi-party computation, homomorphic encryption, or differential privacy in order to get around these problems. These techniques may lessen the performance of the model or the effectiveness of the system, even when they increase the privacy of model updates or guard against hostile users' poisoning attacks. To address this, researchers must work to balance privacy protection against model performance and offer individualized privacy protection. [6]

III. Federated Learning Types and Uses

There are many types of federated learning and over the years they have become more developed. Here we will discuss Model-centric, Data-centric, Cross-silo, Cross-device, horizontal, vertical, and federated transfer learning. According to Gooday, Federated learning can be divided into two basic types - model-centric and data-centric. In model-centric, there is also - cross-device, cross-silo, horizontal and vertical [7].

- Cross-device - Here learning takes place remotely, and the central model gets updated. Larger businesses can handle the problem of scaling. Usually, data is present in a horizontal fashion.

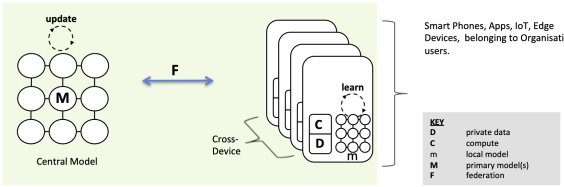
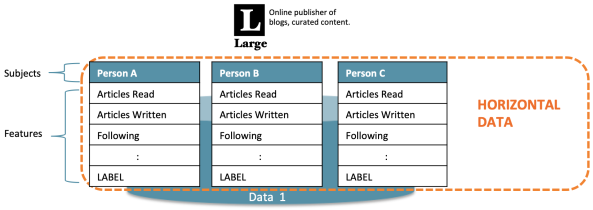


Fig. 1. Cross-device Federated Learning

- Horizontal - In cases where the data share the same feature space but are present in different samples horizontal federated learning can be suited here. This is also known as Homogeneous Federated Learning, it relates to using the same features [8].



Person A	Person B	Person C
Articles Read	Articles Read	Articles Read
Articles Written	Articles Written	Articles Written
Following	Following	Following
:	:	:
LABEL	LABEL	LABEL

Fig. 2. Horizontal Federated Learning

- Cross-silo - Deals with more distributed data present in different organizations or locations. The goal is the same: a central server gets updated, though data is harder to come by due to data security. More scalable and robust computation can be used in each organization eg- Hadoop or Spark clusters.

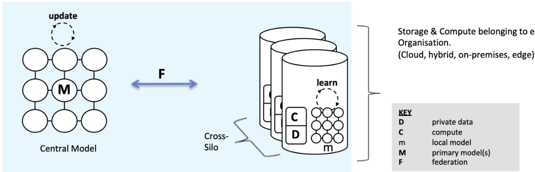


Fig. 3. Cross-silo Federated Learning

- Vertical - It is applicable in scenarios where data shares the same sample ID space but has a different feature space. Also known as Heterogeneous Federated Learning [9].

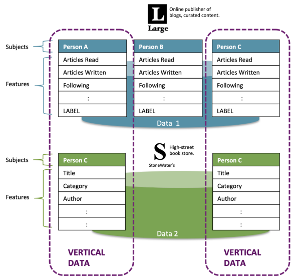


Fig. 4. Vertical Federated Learning

- Federated Transfer Learning - Similar to Convolution Neural Network transfer techniques, but the last few layers have been dropped, the model is re-tuned and the model detects the labels on smaller datasets. FedHealth utilizes this method [10] [11].

- Data-Centric Federated Learning - This is a newer type of federated learning that is more similar to peer-to-peer transfer. In a most likely scenario, the host has data they wish to protect in PyGrid, this would allow anyone to make requests for inference against the data or for training. Tools and techniques are needed to allow adequate data preparation, discovery, and wrangling. While simultaneously limiting, controlling, and overseeing any data leakage [7].

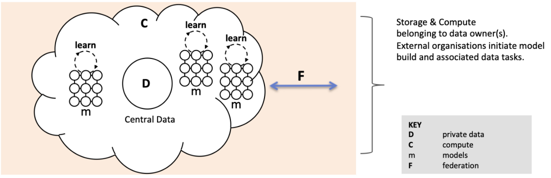

C
learn
learn
learn
D
Central Data
m
m
m
F
Storage & Compute
belonging to data owner(s).
External organisations initiate model
build and associated data tasks.
KEY
D private data
C compute
m models
F federation

Fig. 5. Data-centric Federated Learning

- Other Federated Learning Types - Papers on Self-Supervised, Few-shot learning, and Zero-Shot federated learning are available. Another type is Reinforcement Federated Learning. Also, there is the newly Federated Learning of Cohorts (FLoC).

IV. Popular Federated Learning Technology in Healthcare

Federated learning is a broad topic and there have been many types and discussions over the years. Many institutions and researchers are still updating federated learning with various different technological advancements. Currently, Blockchain, IoT, and network-based FL are used in the industry. Below we discuss them with all the necessary details.

A. Blockchain Based Federated Learning

As per Rifai et al, given a network of peers that have no trust in one another, the blockchain provides a robust way to verify that the data of all peers are identical. One application that has been heavily studied is Electronic Health Records (EHR) management. It is decentralized as users are split into patients, government organizations, and medical organizations. Blockchain solutions allow all users to interact transparently with fair usage consent [2]. Below shows a blockchain-based FL architecture for healthcare.

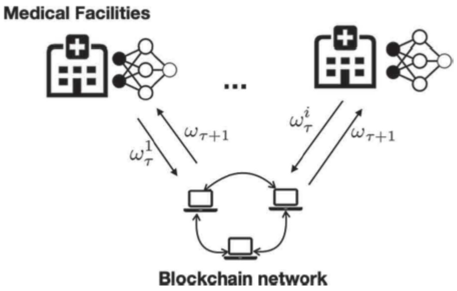


Fig. 6. A Blockchain-based Federated Learning System for Medicine

B. Google's Federated Learning Architecture

As per Treleaven, there are two core aspects of federated learning - data infrastructure - which allows secure communication between collaborators and ensures data does not go out of the owner's control, and machine learning - which enables learning of the data while keeping the sources in their locations. Federated learning ecosystems are of two types as well - On-device- like phones, computers, etc and Inter-Organisational - between organization servers or machines. European MELLODDY is one such project that 10 pharmaceutical companies are collaborating on. The data technologies that participate in information management are digital identifiers (DOI), data standards, data analytics, and data records [4]. Below shows an image of Google's Federated Learning architecture.

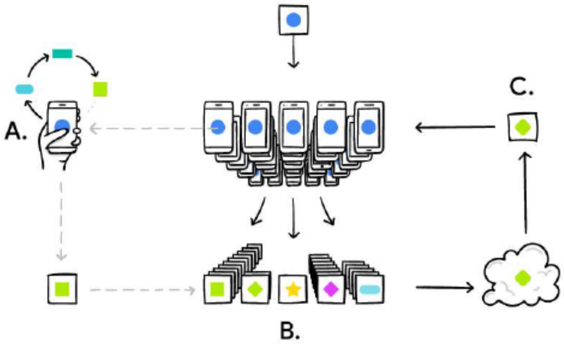


Fig. 7. Google Federated Learning Architecture

C. IoT Based Federated Learning

According to Alawadi et al., due to the increasing recognition of the Internet of Things -IoT, there needs to be more data management systems. These ideas have allowed the usages of wireless devices and monitors to receive data and perform more advanced functions of personal health statuses. There has been an improvement in diagnosis and treatments thanks to IoT. Disease detection has gotten more effective thanks to these advanced algorithms. Although there are many problems that prevent IoT from reaching its full potential [5]. Below shows an architecture of a health monitoring platform.

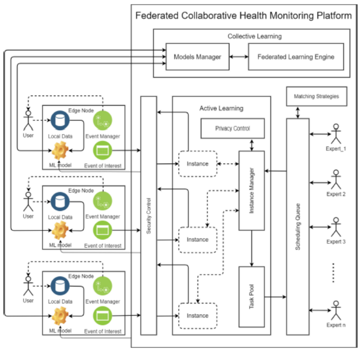


Fig. 8. A Federated Learning Collaborative Healthcare Monitoring System

V. Advantages and Disadvantages of Using Federated Learning in Healthcare

Numerous applications of federated learning are already employed in the healthcare sector. Researchers at Google developed federated learning in 2016 for learning models on mobile devices in a highly distributed environment (McMahan et al. 2016). In this system, an initial model is created by a central server and sent to a few chosen clients for training. Clients call the server with model parameter deltas after some training time, which is then combined and used to update the central model. Numerous times, the procedure is repeated with various clientele. This structure has many benefits for a distributed mobile network, including effective communication and resilience against clients quitting. The federated learning algorithm was specifically created to address the following issues:

- Clients have uneven amounts of data;
- The distribution of data values varies with each client (non-IID data, i.e., not independently and identically distributed);
- The number of clients is high, but everyone's participation is not guaranteed;
- The communication is limited, so minimization of the number of communication rounds is frequently an objective.

In a multiparty situation, as opposed to the conventional federated learning scenario where one service provider links to a loose federation of clients, multiple entities amass data about their clients and aim to improve their data analysis through collaboration. As a result, the following differences from the fully distributed setting are anticipated:

1) Data are much closer to being IID-distributed;
2) The number of participants is limited, but each member's participation can be guaranteed;
3) There are no strict constraints on communication resources;
4) With just a few participants, there is a greater risk of overfitting the global model to local data sets.

As a result, it's possible that some of the federated learning's well-known benefits won't apply in a multiparty situation, thus it's important to carefully evaluate alternative options. First, various collaborative machine learning systems are compared, including alternatives to collaborative learning like training models separately or centralizing the data for model training, in order to determine the benefits of federated learning for healthcare data collaboration. The experiments of McMahan et al. (2016) are replicated in order to determine the circumstances under which the distributed model converges to the global minimum for a small number of cooperating parties and under which it can perform at the level of the nonfederated Performance. Next, functionality that is only provided by federated learning is explored [12].

VI. Prescription Image Based Federated Learning

With all the above said and done, we propose a new idea - on using federated learning in healthcare, for the training of deep learning algorithms from the images of prescriptions. The images can be from a mobile phone, computer, imaging system, etc. The format of the image can be png, jpg, jpeg, or even pdf. The resolution of the image may differ due to the sizes of the devices. Also the larger the image size the sharper the image, but the longer the processing time, due to the presence of more pixels. The federated algorithm will have to take into account all these factors after preprocessing the images to their desired features. Then the training will begin. Firstly the model will be sent to the client devices from the main server. Then the model will take the images from the device of the client and start the image pre-processing. After the pre-processing is finished the machine learning model will begin training locally. After the local training is finished the trained model is sent to an aggregator, then finally the aggregated model is sent to the main server. Below shows the details of the method, which is similar to the ones that are currently available.

Now we discuss the federated learning process, it is similar to the ones done before, but with the added steps of image pre-processing, and semantic analysis for the names, dosages, and types of drugs then the remaining steps are very similar. Below shows the steps in our process.

For the semantic analysis, all the necessary information is taken. Any private information is left out except for the patient's name and registered hospital. The algorithm will be pre-trained with some datasets of drugs that are used in the country. The text is extracted from the images and then the text is classified. After classification, the training begins. According to Jung, Kim, and Jain, the text data present in images contains useful data for automatic indexing, structuring of images, and annotation. Detection, localization, tracking,

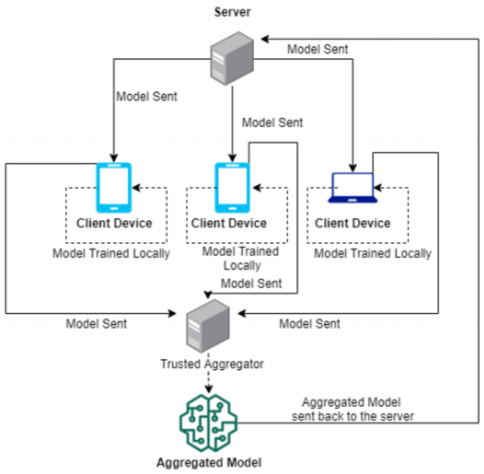
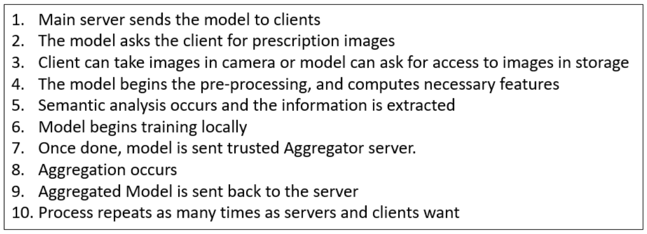


Fig. 9. Diagram of the Federated Learning



1. Main server sends the model to clients
2. The model asks the client for prescription images
3. Client can take images in camera or model can ask for access to images in storage
4. The model begins the pre-processing, and computes necessary features
5. Semantic analysis occurs and the information is extracted
6. Model begins training locally
7. Once done, model is sent trusted Aggregator server.
8. Aggregation occurs
9. Aggregated Model is sent back to the server
10. Process repeats as many times as servers and clients want

Fig. 10. Steps of the Federated Learning Process

extraction, enhancement, and recognition of the text from given images are involved in this process. It is extremely challenging due to variations in text size, style, alignment, orientation, and low image contrast along with complex backgrounds [13]. Below shows how semantic text extraction works. Ours is very similar to the one shown. For now, we are just using images.

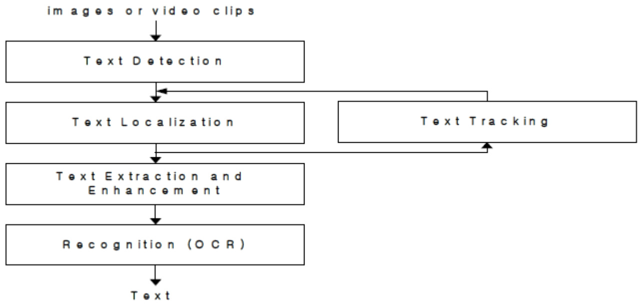
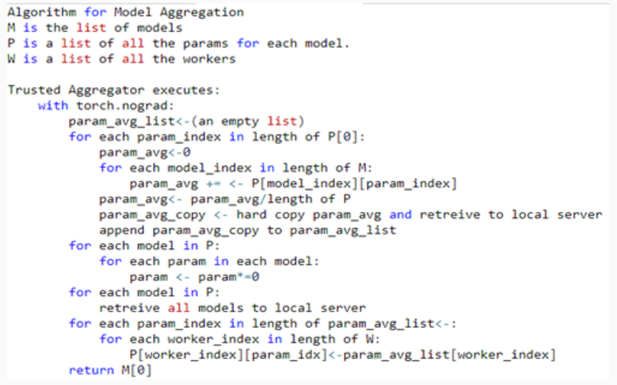


Fig. 11. Semantic Text Detection System

Finally, for the aggregation, we use the pseudo-code given below. This implementation uses synchronous federated learning, therefore all models need to finish their training before being sent to the aggregator. Here federated averaging is used for aggregation. The list of parameters that were saved during model creation will be used to access each of the parameters of each model to get an average of the saved parameters. This can be considered as leveraging transfer learning. Only the last convolutional layer's parameters of all models will be aggregated. Aggregating the other layers will be redundant as the parameters stay the same. To avoid this only the changing layers are taken [14].



```
Algorithm for Model Aggregation
M is the list of models
P is a list of all the params for each model.
W is a list of all the workers

Trusted Aggregator executes:
    with torch.nograd:
        param_avg_list<-(an empty list)
        for each param_index in length of P[0]:
            param_avg<-0
            for each model_index in length of M:
                param_avg += <- P[model_index][param_index]
            param_avg<- param_avg/length of P
            param_avg_copy <- hard copy param_avg and retreive to local server
            append param_avg_copy to param_avg_list
        for each model in P:
            for each param in each model:
                param <- param*=0
        for each model in P:
            retreive all models to local server
        for each param_index in length of param_avg_list<-:
            for each worker_index in length of W:
                P[worker_index][param_idx]<-param_avg_list[worker_index]
        return M[0]
```

Fig. 12. Aggregation Pseudo-code

Again as per Gunasekara, following the pseudo code, above each model's trainable parameter for each position of the parameter is being conjoined together and averaged. The averaged parameter is appended to a new list after being hard copied. After aggregation is finished the new list will have the same length as the number of trainable parameters of one model. The parameters of all individual models are set to zero before being retrieved back to the server. They are set to zero as it will be a breach of privacy to the user's data in the central server [14].

We believe this new federated learning approach can be very useful for finding and classifying medicine. It will make the process more efficient and much faster than traditional methods. It will also speed up the medicine sorting processes as well. It can also assist in faster medicine delivery while simultaneously reducing errors.

Though we know there are some issues with our model concerning - security, privacy, and ensuring that the data is authentic. Also, there is an issue with processing speed and that is dependent on the client's device. To tackle some of them we propose some solutions. For security, we can look into blockchain or use more robust policy methods. For privacy, we can take users' consent multiple times or utilize double authentication factors. To ensure the authenticity of the data we can program the algorithm to detect duplicates and use more detailed semantic detection methods. For the limitation of devices, we can automate the learning process, by accessing the device configuration. Even if the devices do not finish learning at the same time. We can use a data scheduler in the aggregator server to ensure it has all the data before it begins the process. These are some solutions but we can shed light further in the future on more pragmatic solutions. All in all, we believe this new idea can revolutionize the healthcare industry by speeding up the learning process for analysis.

VII. Conclusion and Future Work

In conclusion, we believe that federated learning will bring great strides in innovation and data analysis in healthcare. Thanks to its distributed computing capabilities we can get faster results. The results are also more accurate and the process is more efficient. We have discussed how FL works and how the data is processed. We have also talked about how the industry uses FL for data analysis and processing. We have also talked of other FL uses in medicine. We also spoke of the merits and demerits of using FL on medical datasets. A clearer picture of ethical issues and medical data policies was given. We have discussed our new idea for using federated learning by taking prescription images of clients. Performing pre-processing on them and then training the model first locally then aggregating it to an aggregation server which will send it back to the main server. We believe FL will bring about a data revolution in the world of medicine when it is fully implemented and utilized to its maximum potential. If we can overcome the mechanical, ethical, and procedural complexities FL will bring forth a revolutionary future for healthcare.

In the future, we can talk about federated learning and data scheduling in further detail. We can look for more pragmatic solutions to some of the problems mentioned above. We can also look into semantic text extraction from video for our model. We also wish to see if federated learning can automatically adjust its capabilities by reading the devices, hardware, and software and trying to perform more detailed experimentation. We also wish to know if Federated learning can be used on the go for the collection of medical data samples. The data samples can also be google - sheet questionnaires, private data from blood banks, or even ECG images of patients. Furthermore, we can also investigate the usage of federated learning in the proliferation of various medicinal drugs. There is an ocean of potential for federated learning in the healthcare sector. If we can solve privacy issues and build secure encryption systems, federated learning will spearhead data analysis in the healthcare industry.

References

[1] N. Rieke, J. Hancox, W. Li, and et al., "The future of digital health with federated learning," *npj Digit. Med.*, vol. 3, no. 119, 2020.

[2] O. E. Rifai, M. Biotteau, X. D. Boissezon, I. Megdiche, F. Ravat, and et al., "Blockchain-based federated learning in medicine," *International Conference on Artificial Intelligence in Medicine (AIME 2020)*, pp. 214–224, 2020.

[3] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, p. 19, 2019.

[4] T. Philip, S. Philip, M. Hirsh, and P. Hirsh, "Federated learning: The pioneering distributed machine learning and privacy-preserving data technology." *Computer*, vol. 55, no. 4, pp. 20–29, 2022.

[5] S. Alawadi, V. R. Kebande, Y. Dong, J. Bugeja, J. A. Persson, and C. M. Olsson, "A federated interactive learning iot-based health monitoring platform," *Communications in Computer and Information Science*, vol. 1450, 2021.

[6] T. X. Nguyen, A. R. Ran, X. Hu, D. Yang, M. Jiang, Q. Dou, and C. Y. Cheung, "Federated learning in ocular imaging: Current progress and future direction," *Diagnostics*, vol. 12, no. 11, 2022. [Online]. Available: https://www.mdpi.com/2075-4418/12/11/2835

[7] A. Gooday, "Understanding the types of federated learning," 2020. [Online]. Available: https://blog.openmined.org/federated-learning-types/

[8] "Utilization of fate in anti money laundering through multiple banks," n.d. [Online]. Available: https://www.fedai.org/cases/utilization-of-fate-in-anti-money-laundering-through-multiple-banks/

[9] "Utilization of fate in risk management of credit in small and micro enterprises," n.d. [Online]. Available: https://www.fedai.org/cases/utilization-of-fate-in-risk-management-of-credit-in-small-and-micro-enterprises/

[10] Y. Liu, Y. Kang, C. Xing, T. Chen, and Q. Yang, "A secure federated transfer learning framework," *IEEE Intelligent Systems*, vol. 35, no. 4, pp. 70–82, 2020.

[11] Y. Chen, J. Wang, C. Yu, W. Gao, and X. Qin, "Fedhealth: A federated transfer learning framework for wearable healthcare," *IEEE Intelligent Systems*, vol. 35, no. 4, pp. 83–93, 2020.

[12] A. Bogdanova, N. Attoh-Okine, and T. Sakurai, "Risk and advantages of federated learning for health care data collaboration," *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems Part A Civil Engineering*, vol. 6, no. 3, p. 04020031, 2020.

[13] K. Jung, K. I. Kim, and A. K. Jain, "Text information extraction in images and video: A survey," *Pattern Recognition*, vol. 37, no. 5, pp. 977–997, 2004.

[14] A. Gunasekara, "A federated learning approach for pill identification," 2020. [Online]. Available: https://blog.openmined.org/a-pill-identifier-using-federated-learning/