


# An Empirical Study on Privacy-Preserving Swarm Learning for Cataract Detection



Thilak Shekhar Shriyan, Samyak Maurya, Janavi Srinivasan,  
Vaibhav Guruprasad Achar, Pooja Agarwal, and Arti Arya 

**Abstract** Cataract is one of the most prevalent eye diseases in today's day and age. Roughly 51% of the world's cases of blindness is a result of cataract even though it can be prevented if detected at an earlier stage. This paper proposes a privacy-preserving cataract detection model with a maximum accuracy of 98%, which predicts if a patient has cataract by processing their retinal scan using a decentralized framework called Swarm Learning. The main focus of this paper lies in preserving the privacy of patient data while creating an accurate and robust model. The performance of a machine learning model directly correlates with the amount of training data. Healthcare data is highly distributed in different hospitals, and data privacy laws make it difficult to collect data and train a model in a centralized setup. Hence this work focuses on a decentralized architecture, where each hospital acts as an individual node with its own training data and a VGG-19 cataract detection model. The model proposed in this paper provides promising results even though it contains non-independent and identically distributed data, i.e. the amount of data and the nature of data varies with each node.

**Keywords** Swarm learning · Privacy-preserving machine learning · Decentralized architecture · Cataract detection · Healthcare

## 1 Introduction

Traditional machine learning models are trained in a centralized server, where data from all the clients are collected together and stored. The model is then run on this data. This gave rise to the following problems. (i) A central server acts as a single point of failure. (ii) Communication overhead and network delay between the

---

T. S. Shriyan (✉) · S. Maurya · J. Srinivasan · V. G. Achar · P. Agarwal · A. Arya  
PES University, Bengaluru, India  
e-mail: [thilak.shriyan43@gmail.com](mailto:thilak.shriyan43@gmail.com)

P. Agarwal  
e-mail: [poojaagarwal@pes.edu](mailto:poojaagarwal@pes.edu)

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024  
S. Li (ed.), *Computational and Experimental Simulations in Engineering, Mechanisms  
and Machine Science* 146, [https://doi.org/10.1007/978-3-031-44947-5\\_1](https://doi.org/10.1007/978-3-031-44947-5_1)

client and server. (iii) privacy concerns regarding clients sharing their data with a third-party server.

To tackle the privacy issues related to data sharing, federated learning was introduced, where only the model parameters are shared with the central server, and the whole training process is executed by each participant individually. This approach minimizes data transfer and privacy concerns. The central server aggregates all the model parameters and returns the updates to the clients. The downside is that the aggregator or the central server is still a potential single point of failure, and it is difficult to reach a consensus on a trusted aggregator.

These problems can be tackled by using a completely decentralized framework such as Swarm Learning [1]. Swarm Learning is a decentralized, privacy-preserving Machine learning framework. In this framework, training takes place at the edge where data is readily available. Only the updated model parameters are shared with the peers, and not the data itself. There is no aggregator in this case instead, a node is elected as the leader dynamically in each round and does the job of aggregating. The security of the block-chain platform is used to share the learning's with its peers in a safe and secure manner.

Coming to the healthcare sector, patient data is extremely private and data is distributed in different hospitals. To make an accurate and data-driven prediction for any disease, the model has to see huge amounts of data. This data has to be in real-time and cannot be a static snapshot. These requirements can easily be met by using the Swarm Learning framework on the cataract detection model. Using Swarm Learning, every hospital acts as a single node, producing its own data. In this case, the data is the retinal scan of the patient.

Cataract is an eye condition wherein the lens in the eye becomes cloudy due to the formation of a protein layer [2]. If left untreated, it can gradually lead to blindness [2]. This cloudiness is clearly visible in a retinal scan of the patient. The main contributions of the paper are:

1. Discusses the key differences and research gaps between the existing centralized architecture and decentralized architecture.
2. Proposes to combine a decentralized architecture with swarm learning to achieve privacy for patient data.
3. Experiments on various real-life scenarios to demonstrate the power of swarm learning.

To achieve the above-mentioned points, this paper implements a cataract detection model using VGG-19, a deep convolutional neural network, pretrained on imagenet. All the nodes train locally on their own data with this model and send the model parameter updates to their peers using a blockchain network. In each round, one of the nodes is dynamically elected as the leader and does the job of aggregating. After this, the aggregated model parameters are returned to all the nodes. With every round, the model keeps getting better and reflects real-world data. Even hospitals with less data can manage to have a good global model.

Diseases like cataract, which can be easily corrected if detected at an earlier stage, can make use of Swarm Learning in building an accurate model so that it can assist

doctors in giving quality care and also reduce workloads. Irrespective of the region of hospitals, the nature of the data, or the amount of data available, every hospital should have such a robust cataract detection model.

## 2 Literature Survey

Patil et al. [3] performed a comparative study to identify and classify different techniques to help automate cataract detection. These cataract detection techniques mainly consisted of three main steps that are Pre-processing, Feature Extraction, and Classification. It uses a wide variety of techniques, allowing different steps of this technique to advance. Optic Disks were used to identify the region of interest and edge detection was to identify the drusen. Another technique, the Red Reflex method, was used where patients were kept in a dimly lit room and given eye drops to dilate their pupils. Passing light through the pupils formed an optical pathway, allowing them to examine and capture images. The processing of these images was optimized using Adaboost, allowing the analysis of the iris. KNN was used to differentiate between the uniformity and dissimilarities that appear on the iris using KNN.

Qiao et al. [4] implemented another technique that uses genetic algorithms along with SVM classifiers to classify retinal images. The process is divided into 4 stages where the image was segmented, performed feature extraction on it using histogram equalization, GLCM(Gray Level Co-occurrence Matrix), and wavelet feature extraction to achieve different feature weights. These weights are then fed into the genetic algorithm to find the best representation of the image and use SVM to classify into different levels of cataract with an accuracy of 95% for the same [4].

Weni et al. [5] shifted from a traditional machine learning approach, deep learning methods were implemented for image feature extraction. By altering the number of epochs and minimizing the data CNN allowed to increase the accuracy. Images were collected and augmented, which were then sent into a series of convolution and max pool layers for feature extraction. It uses RELU for the hidden layers and Softmax as the activation function. To speed up the gradient descent, it uses ADAM optimiser and the final loss function was cross entropy, allowing the model to achieve an accuracy of 88%.

Khan et al. [6] extended this method by using VGG-19, by collecting data from Shangong Medical Technology Co. Ltd of around 800 patients. Since it's a pre-trained model, only the hyperparameters of the dense and dropout layers were trained to improve classification accuracy using this method, which increased the accuracy to about 97.47%.

Rieke et al. [7] studied and realized that apart from improving accuracies and advancements in technology, they mention the problems we face challenges in data sovereignty, security and privacy now putting a barrier to sharing data. Federated learning may offer solutions for the long-term problems in digital health and also underline the issues that need to be resolved with it. It is a method that involves collaboratively training the algorithm without actually sharing the data. Instead, only

the parameters are shared with a centralised server; the model is trained locally at each organisation. The participants cannot access data but only the parameters which will be aggregated in the central server. To enhance privacy, approaches like differential privacy or learning from encrypted data have been proposed. Despite these benefits, it cannot solve all problems due to the diverse characteristics and dimensionalities of data. There is a significant trade-off between privacy versus performance.

Verbraeken et al. [8] suggested that we need to use distributed machine learning rather than the traditional centralized machine learning approaches to get past these obstacles. As data production and size rise, it will take longer to train a model with such a large amount of data. In addition to privacy concerns, there are additional overheads to consider with data transfer over the network. Hence, the centralized solution becomes extensively difficult to store and compute, therefore necessary to use a distributed approach providing parallel computation, data distribution, and resilience to failures.

In contrast to a centralized state, a peer-to-peer distributed machine learning model architecture solves the current concerns. As each node is a fully distributed model, it has a copy of the parameters and each worker talks to one another. It allows the system to become more scalable and eliminates a Single Point of failure. Introducing a distributed ensemble model allows it to preserve the privacy of the content, as the model training is completely separated from the result. It makes sure no sensitive data is leaked into the model [8].

Roy et al. [9] developed a new Fed learning framework called BrainTorrent, and it was introduced to overcome the disadvantage of Federated learning of using a central server. By making it completely decentralized, it uses a P2P environment. Participants interact with each other without relying on a central body. On performing experiments and comparing it with Federated learning, it is observed that Dice scores for aggregated models and average Dice score over Clients by gradually increasing the number of clients. It also outperforms Federated learning when introduced with non-uniform data distribution, even with such uneven distribution BrainTorrent aggregates the model and performs better than Federated learning system.

Chen et al. [10] developed LearningChain, which introduces blockchain to create a decentralised machine learning system that protects privacy and is secure. It discusses personal and security threats [Byzantine threats] by analysing various threats. A learning chain is introduced to address them. A node in this framework may function as a computing node, a data holder, or both. It primarily consists of three processes. Initializing the blockchain, computing the local gradient, and aggregating the global gradient are the three steps. Data privacy is achieved through differential privacy, whereas identity privacy is accomplished by giving nodes a pseudo-identity.

Han et al. [1] mention that in real-world scenarios, the majority of the data is stored in a non-IID distributed fashion across various servers and locations. The use of a central server during training raises issues with data ownership, confidentiality, privacy, security, etc. Federated learning reduces some of the worries by addressing confidentiality issues locally, but it runs the risk of over-fitting these models. The star-shaped architecture hurts fault tolerance and still leaves out the central custodian.

Swarm Learning (SL) is the most recent example of cutting-edge decentralised Federated learning. It uses permission blockchain and decentralised hardware to securely onboard members and elect leaders on the fly. Developers can rely on Swarm Learning to achieve similar accuracy to Centralized learning even if the dataset is unbalanced or contaminated. Developers can rely on Swarm Learning to produce results that are more fair than Centralised when the dataset is biased toward irrelevant features. In other words, for the same testing set, models trained on various SL nodes offer comparable accuracy. It enables the models to perform better than other systems and architectures in a variety of areas, including performance, data imbalance, fairness, fault tolerance, scalability, and other factors [1].

Based on investigation and analysis of various methods for detecting cataracts, it is found that there is a tradeoff between privacy and accuracy. This work bridges the research gap of preserving the privacy of patient data in the healthcare sector, allowing multiple healthcare institutions to collaborate and paving a path towards utilizing the power and advantages of decentralized computing and attaining an at-par accuracy with the existing approaches.

### 3 Methodology

Healthcare data is dispersed around numerous hospitals and is thought to be extremely sensitive. This paper has employed a Privacy-Preserving Decentralized Machine Learning framework called Swarm Learning to protect user privacy and utilize varying data for model training.

The following section outlines three elements: Pre-processing, Model Training, and Swarm Integration, which explains the approach taken in this work.

#### 3.1 Dataset Description

The Data set used is the Ocular Disease Intelligent Recognition (ODIR) [11]. The dataset contains a collection of patients data gathered by Shangong Medical Technology Co., Ltd. from various hospitals and healthcare facilities in China. These institutions use a variety of cameras from the market to capture fundus images, producing images with a wide range of resolutions. The dataset includes 5000 patients' retinal images of both eyes from people of various ages and doctors' diagnostic keywords which categorize multiple diseases such as pathological myopia, diabetes, hypertension, age-related macular degeneration, cataracts, and glaucoma among other diseases.

### 3.2 *Data Split and Preprocessing*

The images in the dataset have been resized into  $224 \times 224 \times 3$  as the VGG19 model accepts data from the input channel in the above format. To read the images faster, we have converted the images to NumPy arrays (.npz format). Further, these NumPy arrays are split into training and testing data in the ratio 80:20.

The data splits considered reflects a real-life scenario where data across different organizations (hospitals/clinics) are unequally distributed, containing biased data about a particular region, sex, ethnicity, or even type of organization. Hence, in this paper, we have segregated our dataset into three categories such as Gynac (GY) containing a dataset of all women from the age 18–60, General Physician (GP) containing a dataset of men and women up to the age 60 and Senior Citizens (SC) which contains a dataset of all men and women above the age of 60. These categories are trained separately on each node and results are compared.

### 3.3 *VGG-19 Architecture*

- VGG19 is a variant of the VGG model which consists of 19 layers (16 convolution layers, 3 Fully connected layers, 5 MaxPool layers, and 1 SoftMax layer). The model takes an input image size of  $224 \times 224$  and is a pre-trained model trained on the ImageNet dataset.
- This paper uses a transfer learning approach that froze the pre-trained convolutional layers and trained the fully connected layers with the ODIR dataset.
- Further, to avoid over-fitting, this paper uses Early-Stopping and Dropout Regularization techniques, which compare gradient values of each iteration, and if no significant difference is observed, gradient descent is stopped.
- ADAM optimizer helps to reach convergence at a faster rate by altering the learning rate and utilizing the momentum.
- Binary cross entropy has been used as the loss function as the model predicts only two classes namely, cataract and normal.

### 3.4 *Swarm Learning Integration*

The Swarm Learning framework can be incorporated into the ML model by incorporating the Swarmcallback API. This paper installs the Swarmcallback API separately in each docker container (SL node).

The Swarm Learning framework receives a view of the internal states and statistics of the model during training from the Swarmcallback API. This API performs tasks related to Swarm Learning during training, such as sharing parameters with all network peers after a synchronization interval.

Parameters used in the swarmcallback API include,

- `syncFrequency`: Sets the number of local training batches carried out between two swarm synchronization rounds.
- `minPeers`: Describes the minimum number of SL peers needed for each synchronization round for Swarm Learning to continue.

The patient's data is trained locally on each container having its own model and each of these models produces different model weights. The Swarm Learning framework needs to be configured and up and running before each container can start running the model. Each container is called a node and each node represents an organization (Eye hospital). The models from individual nodes communicate with each other using block-chain and swarm learning network to build a better global model.

Once the parameters are set the interval synchronization takes place, The interval of these syncs can be varied and the number of participating nodes in the synchronization can be controlled.

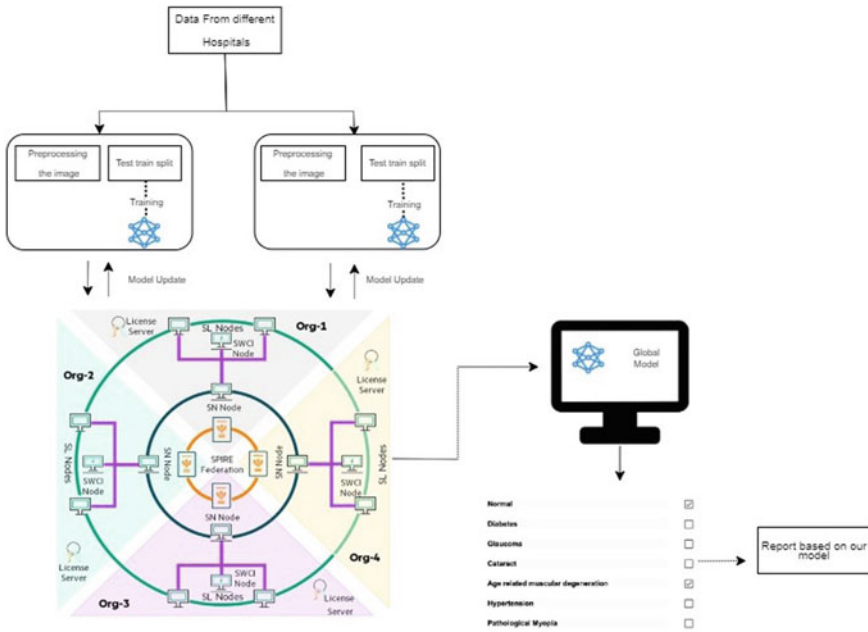
By limiting the number of minimum nodes, If the number of participating nodes fails below the threshold set, the platform will block this synchronization process until it reaches the required range of participating nodes. With the completion of multiple iterations of merging the model parameters, the global model is sent to all the nodes (Eye hospitals) through the block-chain network for use.

### ***3.5 Proposed Workflow***

As shown in Fig. 1, the machine learning model residing in each hospital organization takes in the pre-processed retinal images as input and the VGG-19 model begins training on them. Once the model has trained the weights, bias, and parameters it is passed onto the SL (Swarm Learning) node. The SL node then participates in the merging process and the updated parameters are fed back to the VGG-19 model. The SN (Swarm Network) nodes are responsible for saving internal states to the Ethereum blockchain network and the process can be specified by using the arguments from the SWCI (Swarm Learning Command Interface) node. The learned weights are then fed back to the VGG-19 model and can thus be used to classify new retinal images as cataracts or normal.

## **4 Experimental Setup**

In this section, the paper elaborates the experimental setup considered, to demonstrate the power of Swarm Learning, by comparing it against a centralized machine learning setup in a real-world scenario.



**Fig. 1** The proposed approach for cataract detection using swarm learning framework

Hospitals have highly diverse data as each patient can be considered a single data source. Each hospital, clinic, department, or research lab can be viewed as a single node. Hence the data corresponding to each node can be different. For example, in a gynecology department, the patient data will majorly correspond to the female population between the age group of 18–50. A model pertaining to a single node in such a case, could highly overfit the training data and hence perform poorly on the test data.

To elaborate further, let us consider a clinic present in a rural area, which has significantly less training data considering they have insufficient means for data collection. Training a model in a centralized way in this case also will give an undesired accuracy. For these situations, collaborative learning outperforms centralized machine learning.

This paper demonstrates these results by considering the following data splits, namely the gynecology department, general ward, and senior citizen, and training them in both a centralized and decentralized fashion. The following are a few things to note regarding the experimental setup and system configuration.

1. The gynecology department has data majorly coming from women between the age of 18–50.
2. The general ward has data points of all the patients irrespective of their age and gender.



**Table 1** Accuracy obtained under multiple experiments

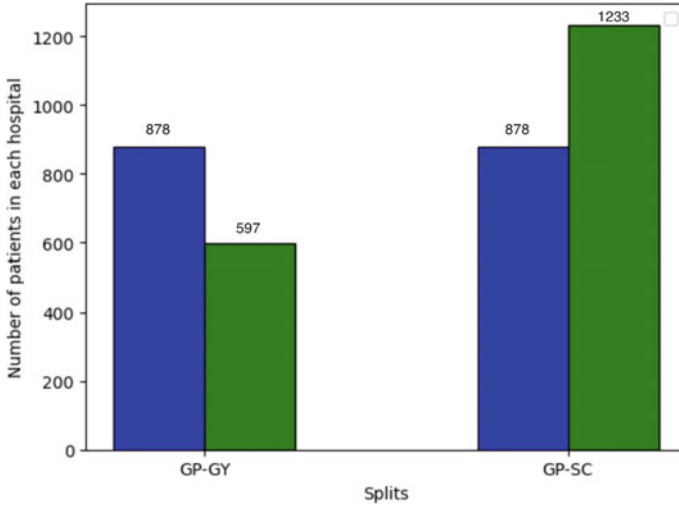
Experiments	Model accuracy		
	General physician (GP)	Gynac (GY)	Senior citizens (SC)
Centralized model	93.9	93.3	97.7
Swarm learning GP-GY split	95.48	95.48	–
Swarm learning GP-SC split	98.27	–	98.27

3. The senior citizen data is assumed to come from old age homes where the patients are above the age of 60.
4. The number of swarm learning nodes is 2.
5. Each swarm learning node is a Linux machine with 4GB RAM having its own training data.
6. Train test split is 80–20.
7. This paper considers two different scenarios with the splits for the training data as mentioned below (Fig. 2).
  - (a) General population-gynecology department (GP-GY) split.
  - (b) General population-senior citizen (GP-SC) split.
8. The test data used to validate the model is the same throughout all the splits.
9. 10 swarm learning iterations were conducted for the GP-SC split.
10. 8 swarm learning iterations were conducted for the GP-GY split. Lesser number of iterations were conducted due to lesser data points in this split.

## 5 Results and Discussion

From Table 1, it can be seen that after carrying out the training process for all the splits using the centralized and Swarm Learning model and testing them, the maximum validation accuracy obtained under the Swarm Learning setup is 95.48 and 98.27% for GP-GY and GP-SC splits respectively. On the other hand, the maximum validation accuracy obtained for the centralized setup is 93.9, 93.3, and 97.7% for GP, GY, and SC nodes respectively.

Cataract is a disease that is more common among older people, i.e. senior citizens. Hence it is obvious that the data points corresponding to senior citizens will be the most in number, followed by the General population. The gynecologist ward has the least amount of data points. From the table, we can clearly see that senior citizen performs fairly well in a centralized setup, but the accuracy of the gynecology department and the general population is not up to the mark. Using swarm learning, in the first split GP-GY, the ratio of data points is approximately 60–40. The general



**Fig. 2** Skewness of data in each node for both the splits

population node shares its learning with the gynecology node and their accuracy becomes progressively better with each iteration. After 10 iterations, it is observed that the collaborative learning accuracy is better than their individual node accuracy. For the second split GP-SC, the ratio of data points is approximately 30–70. Even though the senior citizen node gave a good enough accuracy in a centralized setup, due to its large number of data points, swarm learning still outperforms this.

Figure 2 shows the number of data points for each split. It can be observed that even with unequal data points in each node, i.e one node has significantly more data points than the other, the global model still turns out to be good for both nodes. This happens because the model corresponding to the node with lesser data points learns from the node corresponding to more data points.

Figure 3 shows the superiority of swarm learning in comparison to centralized learning. It can be observed that the swarm learning accuracy of GP-GY split beats the accuracy obtained by the centralized architecture with various splits. This is true in the case of GP-SC split as well.

Figures 4 and 5 show the confusion matrix of both the swarm learning splits. Recall obtained for the GP-GY split is 90% and recall obtained for the GP-SC split is 95%.

After conducting experiments on various real-life scenarios, it can be clearly derived that swarm learning is highly useful in situations where the nodes need to learn collaboratively and help those nodes with scarce data due to poor data collection mechanisms, achieving good accuracy.

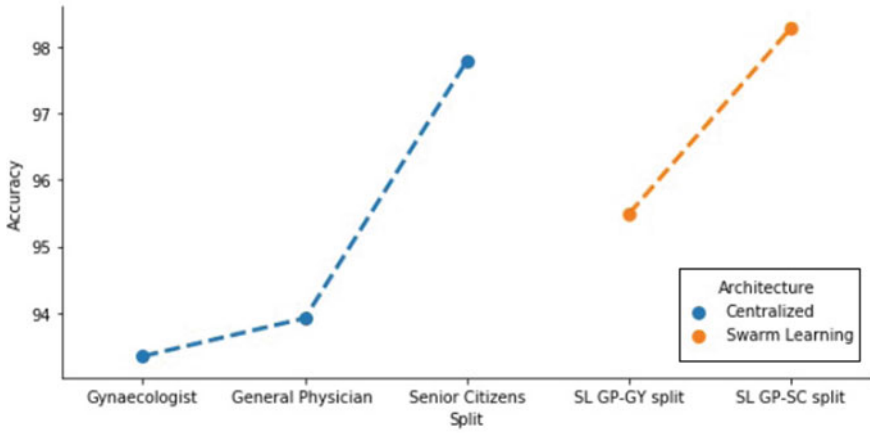


Fig. 3 Accuracy comparison between centralized and swarm learning architecture

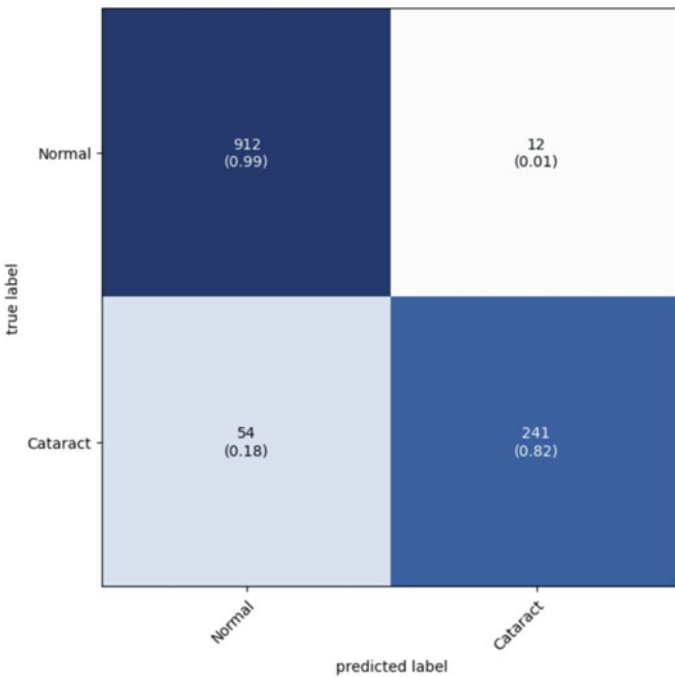
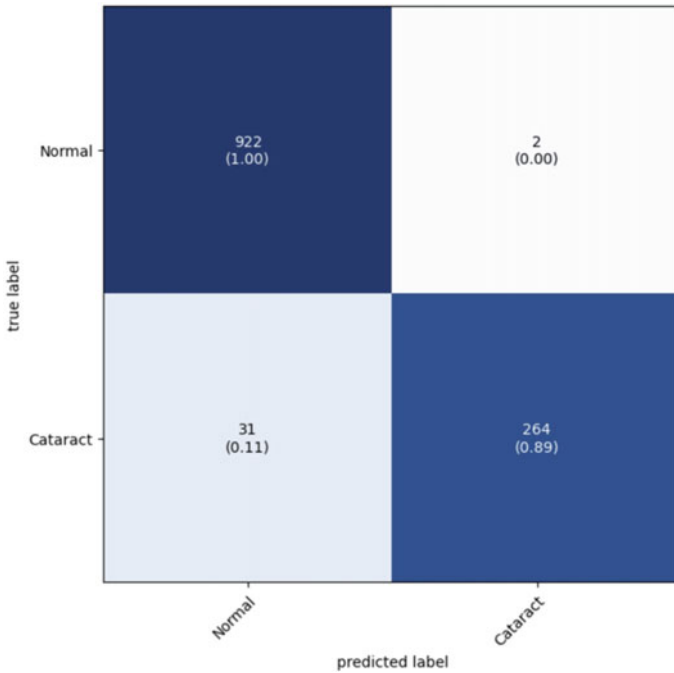


Fig. 4 Swarm learning: confusion matrix for GP-GY split and recall of 90%



**Fig. 5** Swarm learning: confusion matrix for GP-SC split and recall of 95%

## 6 Conclusion and Future Scope

This paper proposes a novel approach of combining Swarm learning with cataract detection model to preserve the privacy of patient data. The experiments conducted demonstrate that Swarm Learning is advantageous even in a non-independent and identically distributed setting with scarce data. User privacy can be achieved with the aid of a permissioned blockchain without the need for additional payload on the machine learning model, and a global model can be shared among all participating peers, with each peer contributing to the updating of the model parameters.

Experiments carried out in this work are limited to two swarm learning nodes. With sufficient resources, the number of nodes in this work can be increased. It is also possible that the data collection methodologies of a few hospitals or nodes may be flawed resulting in noisy data. If experiments are carried out in such a case, it should be ideal that the nodes with good data points improve the overall accuracy of the model. Furthermore, this work can be open to multi-class detection of other important retinal diseases such as Glaucoma, Hypertension, and Diabetes.

**Acknowledgements** We sincerely thank and appreciate Mr. Ravi Sarveshwar, Master Technologist, ADC and Mr. Dharmendra, Section Manager, ADC from Hewlett Packard Enterprise for their constant support during the entire course of this work. Their suggestions and feedback on the work carried out were invaluable in producing this paper.

## References

1. Han, J., et al.: Demystifying swarm learning: a new paradigm of blockchain-based decentralized federated learning. arXiv preprint [arXiv:2201.05286](https://arxiv.org/abs/2201.05286) (2022)
2. Xu, X., et al.: A hybrid global-local representation CNN model for automatic cataract grading. *IEEE J. Biomed. Health Inf.* **24**(2), 556–567 (2019)
3. Patil, D., et al.: Analysis and study of cataract detection techniques. In: 2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC). IEEE (2016)
4. Qiao, Z., et al.: Application of SVM based on genetic algorithm in classification of cataract fundus images. In: 2017 IEEE International Conference on Imaging Systems and Techniques (IST). IEEE (2017)
5. Weni, I., et al.: Detection of cataract based on image features using convolutional neural networks. *Indones. J. Comput. Cybernet. Syst.* **15**(1), 75–86 (2021)
6. Khan, M.S.M., et al.: Cataract detection using convolutional neural network with VGG-19 model. In: 2021 IEEE World AI IoT Congress (AIIoT). IEEE (2021)
7. Rieke, N., et al.: The future of digital health with federated learning. *NPJ Digit. Med.* **3**(1), 1–7 (2020)
8. Verbraeken, J., et al.: A survey on distributed machine learning. *ACM Comput. Surv. (CSUR)* **53**(2), 1–33 (2020)
9. Roy, A.G., et al.: Braintorrent: a peer-to-peer environment for decentralized federated learning. arXiv preprint [arXiv:1905.06731](https://arxiv.org/abs/1905.06731) (2019)
10. Chen, X., et al.: When machine learning meets blockchain: a decentralized, privacy-preserving and secure design. In: 2018 IEEE International Conference on Big Data (Big Data). IEEE (2018)
11. Larxel: Ocular Disease Recognition. Kaggle, 24 Sept 2020 [Online]. Available: <https://www.kaggle.com/datasets/andrewmvd/ocular-disease-recognition-odir5k>