# Application of federated learning in a healthcare setting

**Ó Fithcheallaigh, S.1, Last Name, Initial.2 (please underline presenting author)**

1 Ulster University, Belfast

2 Institution of second author

*email: o\_fithcheallaigh-s@ulster.ac.uk*

# Introduction

Recent years have seen a marked increase in the adoption of the Internet of Things (IoT) – the network of physical objects that collect and exchange data. As the number of IoT devices increases, the amount of data being collected and stored is also increasing. This increase in the amount of data, alongside improvements in computing power, has contributed to the recent advancements in Artificial Intelligence (AI). Increased data allows for the training of more complex AI models, while more powerful computers have enabled the processing of massive amounts of data which are required for these models. Another growing trend is an increase in public concern over data privacy. According to a Pew Research Centre survey carried out in America, 79% of adults were concerned about the way their personal data was being used by companies [1]. Furthermore, according to the Unted Nations Conference on Trade and Development (UNCTAD), 137 out of 194 countries have put in place some form of legislation to protect privacy and data[[1]](#footnote-2).

A diagram of a flowchart

Description automatically generated

***Figure 1*** *Federated Learning Systems Diagram*

Recently, researchers working in AI have been looking for ways to ensure data privacy in their models, while still being able to benefit from the increasing amounts of data. One approach that shows promise is Federated Learning (FL) [2].

This work aims to provide an overview of FL and how it can be applied to the healthcare sector as a way of benefitting from advances in AI, while ensuring data privacy for the users of the services provided.

# Discussion

Taking the example of disease detection, with machine learning (ML), a typical workflow would be to gather the dataset, build and tune a model, deploying it when a desired level of accuracy is reached. But this dataset may be quite old or may not have been updated with the most recent data and is not local to the hospital.

FL offers a way to continually update the ML model while keeping data private. This is done by training a local model on the data held by the health centre (i.e., client). This means that the data never leaves the location. When the local model has been trained, the updated model parameters, and not the data itself, are sent back to a central server, which receives the updates from many sites, and aggregates them to train a new global model which is then sent back to the clients. This process is shown in Figure 1. This process is repeated over a number of iterations, until a desired level of accuracy is reach.

# CONCLUSION

In a healthcare environment, FL offers a way to train ML models which can be widely used on data that remains local to the hospital or health centre, thereby allowing more users to benefit from a system trained on the most recent data.

# References

[1] Engström (*et al.),* Computers in Human Behavior Reports, Vol 9, 2023

[2] McMahan (*et al.),* Artificial Intelligence and Statistics, pp. 1273-1282, 2017

1. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide [↑](#footnote-ref-2)