# The potential of Federated Learning in Healthcare settings

**Ó Fithcheallaigh, S.1, Nugent, C.1, Liu, J. 1, Cleland, I.1**

1 School of Computing, Ulster University, Belfast

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

# Introduction

The increased adoption of internet connected devices, known as the Internet of Things (IoT) has driven both advances in artificial intelligence (AI), thanks to vast amounts of data and processing power now available to researchers, and public concerns over data privacy, with a Pew Research Centre survey finding that 79% of American adults are concerned with how their personal data is being used by companies [1]. As AI researchers look to balance the need for technological advancement with the desire for privacy, federated learning (FL) [2] has emerged as a possible solution.

FL is a type of machine learning (ML) architecture made up of many local clients, and a central server. In FL, the central server transmits an initial model to the clients. The clients will gather data and train the model locally – each client will train its own model on its own data, thereby keeping the data private. Clients can be something as small as a smart watch, or as large as a hospital. Once a client has trained its model on the local data, the model updates are transmitted to a central server, not the data itself. When all selected clients have transmitted their updates, these are aggregated into a new global model which is transmitted back to the clients. This process is repeated until a desired level of performance has been reached. Whilst FL provides great potential in protecting privacy in a healthcare setting, there remains a number of open research challenges. This aim of this paper is to discuss these challenges.

# Potential of FL in healthcare

Given the ability for FL to keep client data private, there is now the potential to use sensitive data held by a health centre to improve outcomes for patients. An example of this is using FL models to improve disease prediction, for example in detecting cancers through an analysis of medical images. Using FL allows for datasets to be continually updated with the latest scans, whilst keeping the scans themselves private. Another area is drug discovery through identification of patterns found in patient’s genetic makeup as well as their medication plans and responses to treatments. Then there is personalised federated learning (PFL), where a model is refined for the purpose of customising it to the unique traits and needs of an individual client [3]. An example of PFL is the development of a system to aid in the diagnosis of Parkinson’s disease by using data gathered by an application on a patient’s smartphone which gathered data on the motor symptoms usually associated with Parkinson’s disease [4].

# challenges in fL

While FL shows promise in several areas, there are still open challenges summarised in Figure 1 [5]. FL brings about significant challenges in terms of data and system heterogeneity. Heterogeneity is introduced by differences in data distributions across clients/servers, or by differences in the architecture of devices involved in the learning process. Heterogeneity can have a negative impact on model convergence and accuracy. Additionally, constant communication between the clients and server can be expensive, and depending on the network topology the communication bandwidth can be limited, which can lead to bottlenecks. Working with multimodal data poses another challenge – what impact will data from various sources (audio, video, numerical data) have on the ability of a FL system to learn and produce accurate models?

A diagram of a learning structure

Description automatically generated with medium confidence

***Figure 1*** *Challenges in Federated Learning*

# CONCLUSION

The challenges found in FL will form the basis of this PhD research. Addressing these challenges should allow for improved performance and great adaption of FL in areas of sensitive 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.

[3] Fahad Sabah (et al.), Expert Systems with Applications, Vol. 243, 2024.

[4] Yiqiang Chen (et al.), IEEE Intelligent Systems, Vol. 35, Issue 4, 2020.

[5] Badra Souhila Guendouzi (et al.), Journal of Network and Computer Applications, Vol. 220, 2023.