# 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

With increased adoption of internet connected devices, known as the Internet of Things (IoT), advancements in artificial intelligence (AI) are accelerating due to increase data and processing power available to researchers. However, this progress is accompanied by an increase in public concern over data privacy, with a Pew Research survey showing 79% of Americans are concerned about how their personal data is used [1]. As AI researchers look to balance technological advancement with the desire for privacy, federated learning (FL) [2] has emerged as a possible solution. FL is a 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 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, avoiding transmission of the data itself. When all selected clients have transmitted their updates, they 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. Despite FL’s potential in protecting privacy, a number of open challenges remain, which this paper aims to introduce and discuss.

# Potential of FL in healthcare

By maintaining data privacy, FL opens the possibility of using sensitive client data to improve patient outcomes. One example is using FL to analyse medical images to improve disease prediction, i.e., cancer detection. 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 smartphone application used by patients to aid in the diagnosis of Parkinson’s disease by gathering data on the motor symptoms usually associated with the condition [4].

# challenges in fL

While FL shows promise in several areas, there are still open challenges [3,5], summarised in Figure 1. FL brings about significant challenges in terms of data and system heterogeneity. Heterogeneity is introduced by differences in data distributions across clients or server, or by differences in the architecture of the devices involved in the learning process. Heterogeneity can have a negative impact on model convergence and accuracy. Frequent client-server communication can be expensive, and limited bandwidth can lead to bottlenecks. Inefficient communications schemes will also increase the negative impact the system has on the environment. 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 challenge

Description automatically generated

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

# CONCLUSION

This PhD research will initially focus on identifying critical challenges in FL, then aim to develop innovative solutions that improve performance and adoption, especially in privacy sensitive domains.

# 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.