# A Hybrid Quantum Neural Network for Split Learning

Hevish Cowlessur[1, 2] Dr. Chandra Thapa[2] Prof. Tansu Alpcan[1]
Dr. Seyit Camtepe[2]
[1]Department of Electrical and Electronic Engineering, University of Melbourne
[2]Data61, CSIRO

**Abstract**

Research in Quantum Machine Learning (QML) has shown its potential in diverse domains such as finance, drug discovery and optimization. Exploring its application in a cloud-like environment, e.g., Split Learning (SL), presents great promise but demands further investigation. SL is a distributed machine learning (ML) approach that allows resource-constrained clients to train ML models collaboratively with a central server, reducing computational overhead and preserving data privacy by avoiding sharing raw data with the server or other clients. While splitting pure Quantum Neural Networks (QNNs) has been studied, the problem remains open and impractical for resource-limited clients lacking quantum computing capabilities. Furthermore, a key concern in SL is data leakage during intermediate data transfers between clients and the server, which can lead to reconstruction attacks compromising data integrity.

By applying the concept of Hybrid QNN in the SL domain, we propose, for the first time to our knowledge, Hybrid Quantum Split Learning (HQSL). HQSL enables classical clients to collaboratively train ML models with a hybrid quantum server and addresses reconstruction attacks in SL. Specifically, HQSL consists of a classical neural network on the client side of SL, while the server side comprises a quantum node followed by classical layers. The quantum node employs a 2-qubit low-depth quantum circuit equipped with the data re-uploading scheme, making HQSL potentially suitable for near-future quantum devices.

Experiments on five datasets of different categories (e.g., image, multivariate, audio) demonstrated HQSL's feasibility and ability to enhance classification performance compared to its classical counterpart. Notably, HQSL achieved mean improvements of over 3% in both accuracy and F1-score on the Fashion-MNIST dataset and 1.5% in both metrics for the Speech Commands dataset. We expanded our studies to involve up to 100 clients, confirming HQSL's scalability. To address the problem of reconstruction attacks, we designed a Laplacian noise layer as a defence mechanism to obfuscate the intermediate data before they are transferred to the server-side model or an adversary's reconstruction model. Empirically, reconstruction attacks were less successful in the hybrid setting than in the classical setting. Despite the noise perturbation, a consequence of the noise defence layer, HQSL maintained higher and more robust classification performance than traditional SL.

Overall, the proposed HQSL allows classical clients to collaboratively train their models with a hybrid quantum server, improving model performance and security against reconstruction attacks. Moreover, HQSL's use of only a small quantum circuit suggests a feasible implementation on near-term quantum computers.

**Keywords**: Quantum Neural Network, Split Learning, Data Leakage in Split Learning, Reconstruction Attacks, Data Re-uploading