A Hybrid Quantum Neural Network for Split Learning

Hevish Cowlessur[1,2], Chandra Thapa[2], Tansu Alpcan[1], Seyit Camtepe[2]

1. Department of Electrical and Electronic Engineering, The University of Melbourne, VIC 3010, Australia
2. CSIRO's DATA61, Sydney, Australia

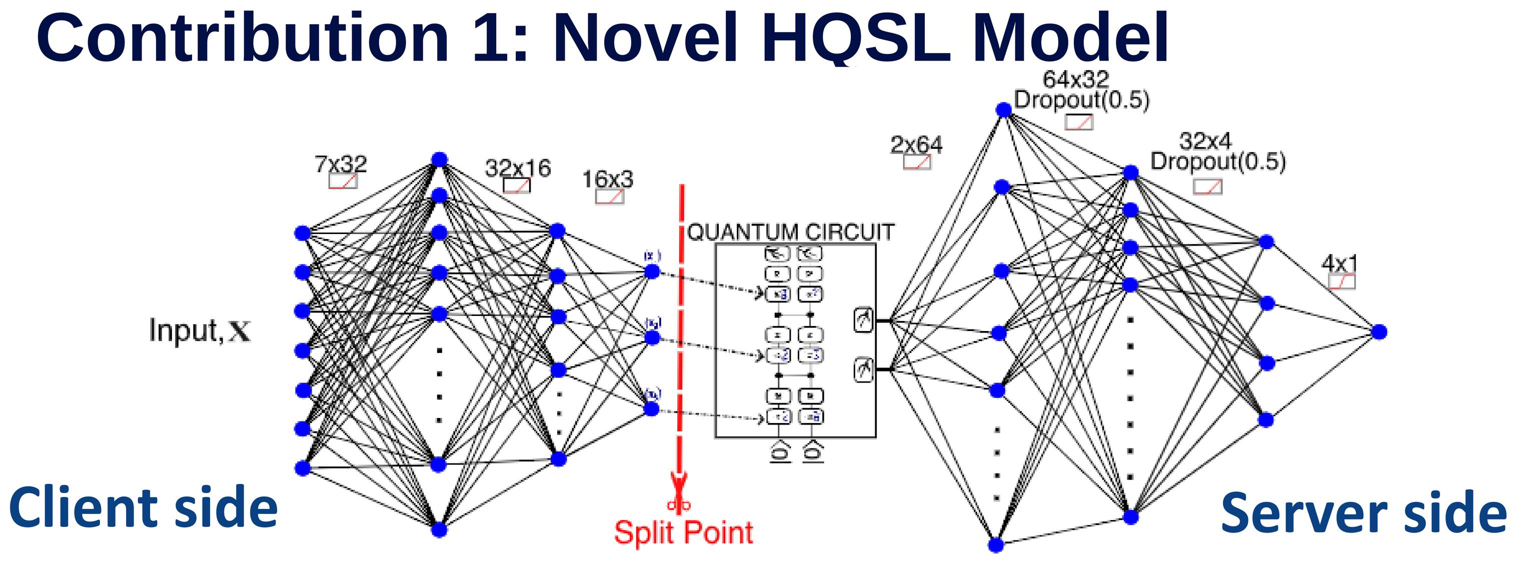
Introduction

- **Hybrid Quantum Neural Networks (HQNN):** Potential to enhance Machine Learning in the noisy intermediate-scale quantum (NISQ) era.
- **Resource-Constrained Clients:** In general, clients (e.g., IoT devices) lack direct access to quantum hardware.
- **Split Learning (SL):** Allows clients to collaboratively train a shared model without high computational demands or exposing raw data.
- **Data Privacy Concerns:** However, split learning models are vulnerable to data privacy leakage and reconstruction attacks.

- **Research Questions addressed in this work:**

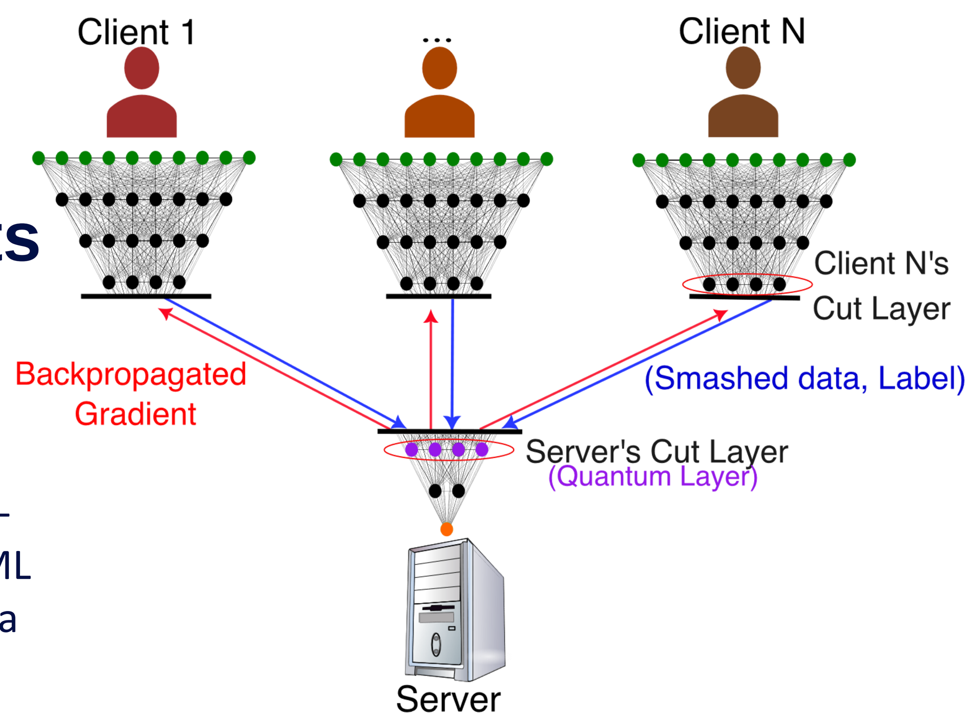
1. *How can SL enable resource-limited clients to benefit from quantum computing?*
2. *How can Hybrid Quantum SL (HQSL) models be secured against privacy threats?*

Contribution 1: Novel HQSL Model



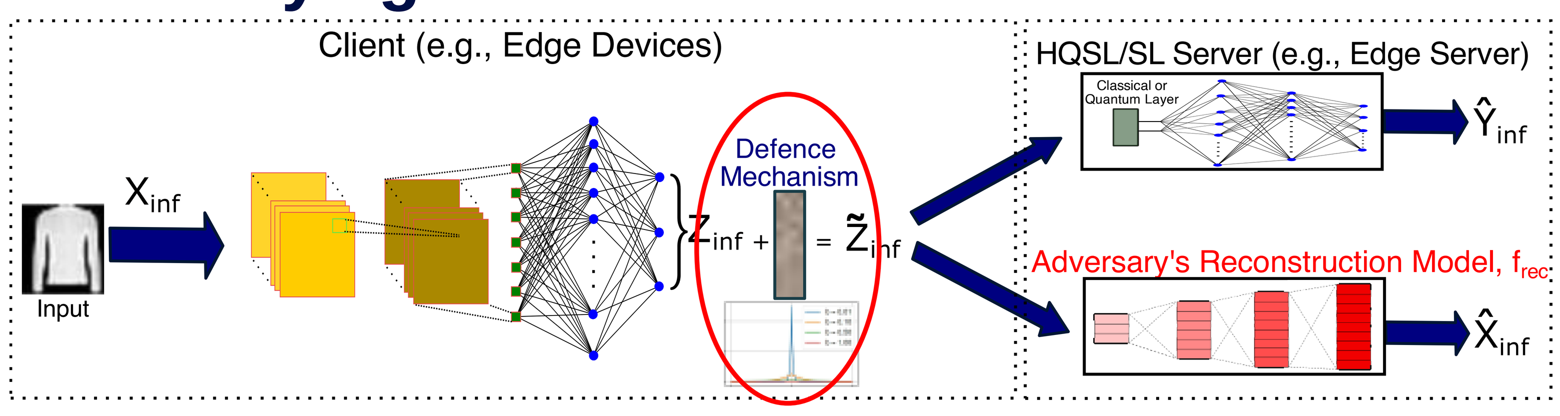
- HQSL consists of an HQNN split into a classical model portion on the resource-constrained client side (**left of split point**), and an HQNN model with a quantum layer, followed by classical layers on the server side (**right of split point**).

Contribution 2: Scaling HQSL for Multiple Clients



- Quantum layer on the server side allows multiple resource-limited clients to train their ML models in collaboration with a hybrid quantum server.

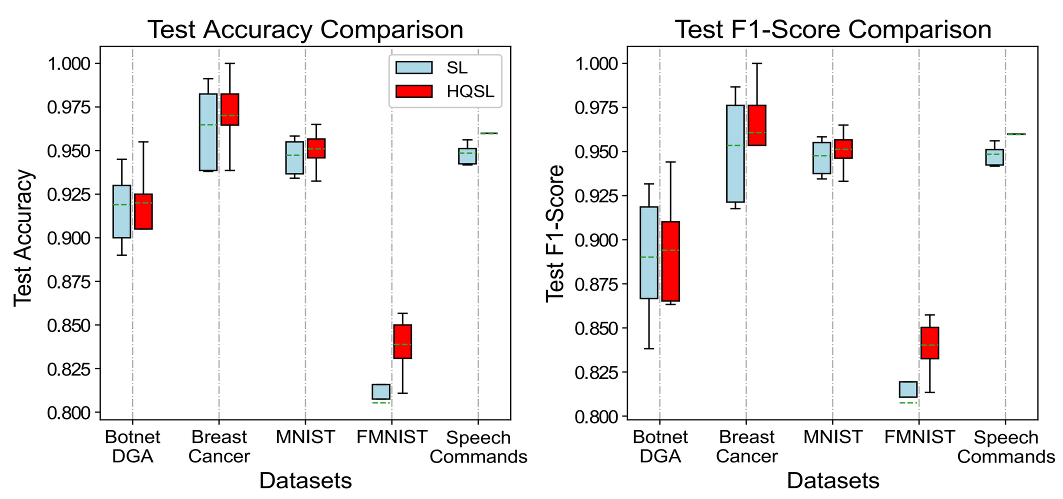
Contribution 3: Strengthening HQSL's Security against Reconstruction Attacks



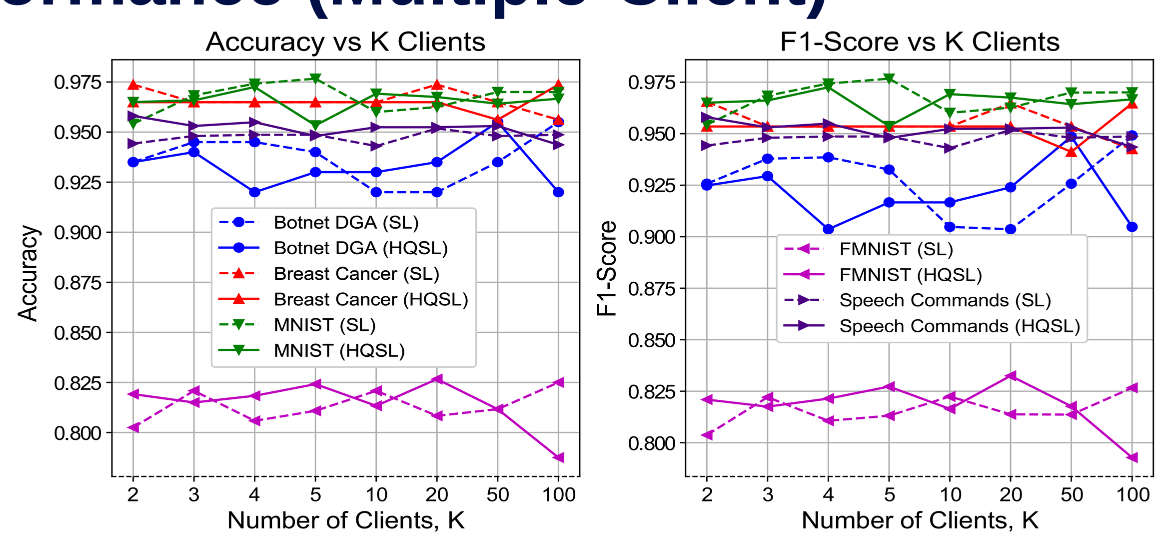
- Defence mechanism consists of a Laplacian Noise Layer at the end of the client side, designed *based on the periodicity of encoding gates of the quantum layer on the server side*. This is the key method we use to make HQSL more robust to data privacy leakage compared to its classical counterpart.

Comparison of HQSL vs SL's Classification Performance (Single-Client)

- **HQSL** with a single quantum layer consisting of a small quantum circuit outperforms its classical counterpart (**SL**) for all datasets experimented with.



Comparison of HQSL vs SL's Classification Performance (Multiple-Client)

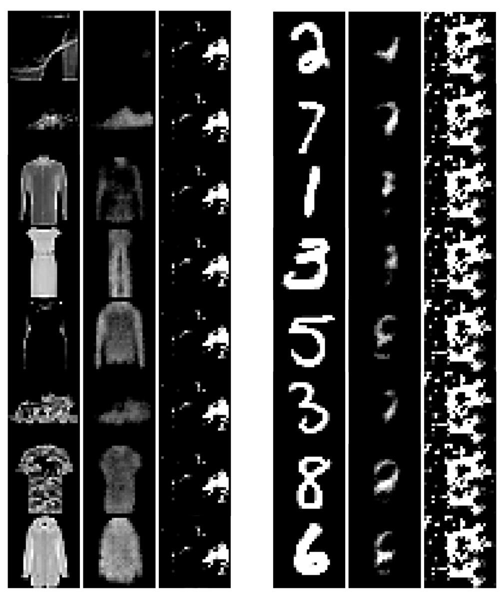


- HQSL performs well even when scaled to accommodate multiple clients.

Comparison of Reconstruction Performance in Hybrid vs Classical Settings

- Using 4 image comparison metrics, we tuned the Laplacian noise parameters making HQSL **more robust** to reconstruction attacks in split learning than its classical counterpart.

- The figure demonstrates reconstruction performance on original images (left) under classical (middle) and hybrid settings (right).



Discussions and Conclusions

- Our experimental results illustrate the feasibility of Hybrid Quantum Split Learning (HQSL) as a means for enabling resource-constrained classical clients to collaboratively train machine learning models with a hybrid quantum server. This approach presents the potential to leverage quantum advantages, notably in enhancing classification performance.
- Also, our proposed defence mechanism makes HQSL more robust against reconstruction attacks on split learning models.
- This work paves the way for future research involving collaborative learning between the classical and quantum domains, for both NISQ and fault-tolerant quantum era.

Link to Paper:

My LinkedIn:

Let's connect!

H. Cowlessur, C. Thapa, T. Alpcan, S. Camtepe, A Hybrid Quantum Neural Network for Split Learning, 2024. https://arxiv.org/abs/2409.16593. arXiv:2409.16593