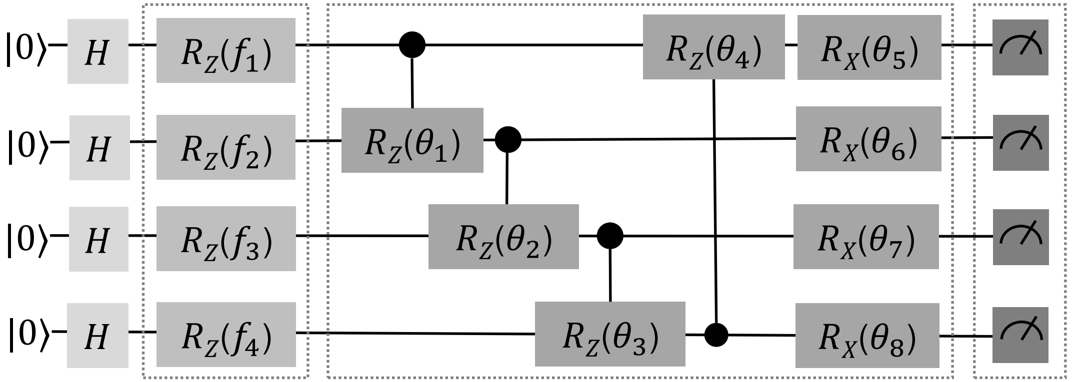
SoK: Security Concerns in Quantum Machine Learning as a Service

Satwik Kundu, Ph.D. Candidate, Penn State
satwik@psu.edu
Advisor: Dr. Swaroop Ghosh

PennState

Quantum Neural Networks

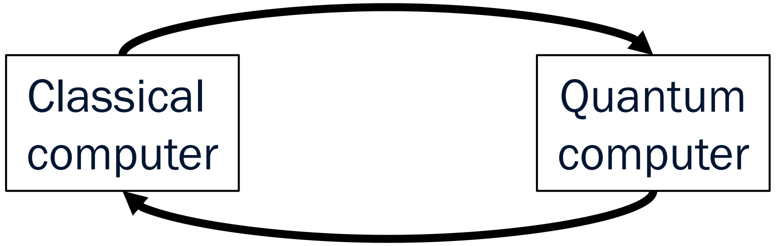
Parameterized Quantum Circuit (PQC)



Encoding

Measurements

QNN with new
set of parameters



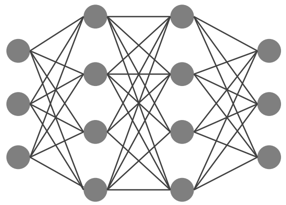
Measured outputs

A classical optimizer (gradient-based/gradient-free) updates the trainable parameters ($\theta_1 - \theta_8$) to generate a desired output distribution.

Classical vs Quantum?

Learning with Classical Hardware	Learning with Quantum Hardware

An example of Neural Network (NN)



1) Two Hidden(H) layers:

40 weights and 11 biases.

2) Input layer:

3-dimensional real vector space.

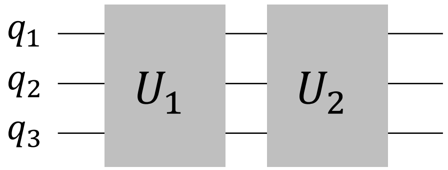
3) Matrix operation (first H layer):

$\boldsymbol{z} = \boldsymbol{x} \cdot \boldsymbol{w} + \boldsymbol{b}$, where $\mathbf{w} \in \mathbb{R}^{3\times 4}$, $\boldsymbol{b} \in \mathbb{R}^4$

4) Non-linearity:

Activation like sigmoid $s(x) = \frac{1}{1+e^{-x}}$

An example of Quantum NN



1) Two Unitaries:

Can have 3 parameters each.

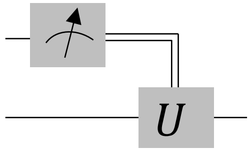
2) Input layer:

2^3-dimensional complex vector space.

3) Matrix operation (U_1):

$$|\psi_1\rangle = U_1|\psi_0\rangle, \text{where } \mathrm{U}_1 \in \mathbb{C}^{2^3\times 2^3}$$

4) Non-linearity:



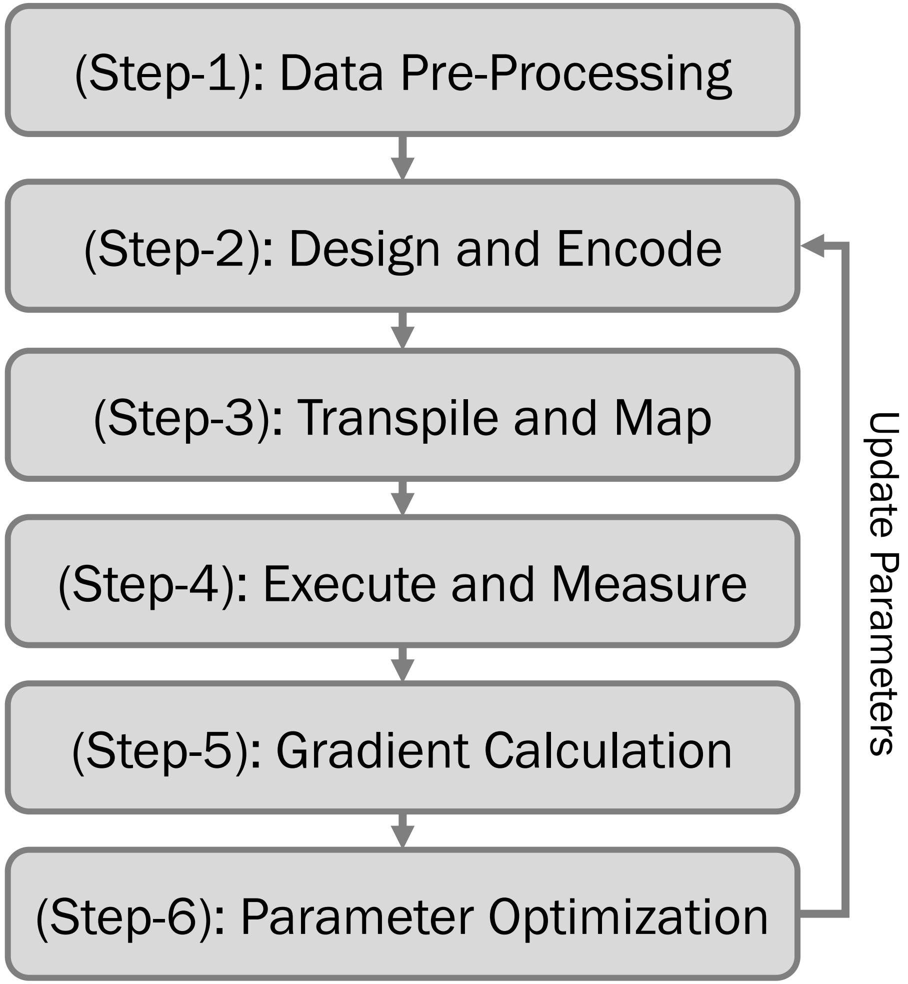
Measurement and conditioned unitary.

Arthur Pesah, et al. "Absence of barren plateaus in quantum convolutional neural networks." Physical Review X 11.4 (2021): 041011.

Quantum Cloud Services

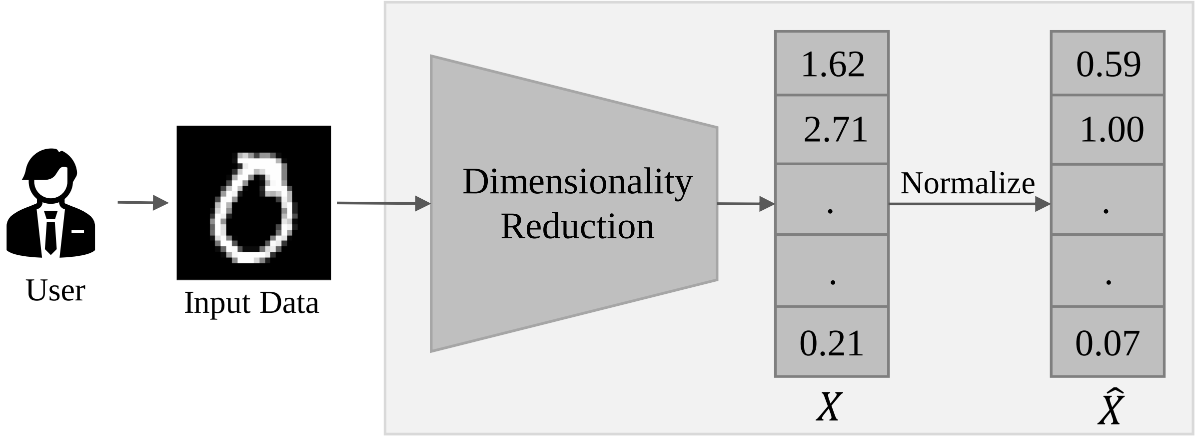
Provider	Qubit Technology	Cost
IBM Quantum	Superconducting	$1.6/sec
rigetti	Superconducting	$0.00090/shot + $0.30000/task
OQC	Superconducting	N/A
IQM	Superconducting	$0.00145/shot + $0.30000/task
QuEra Computing Inc.	Neutral Atom	$0.01000/shot + $0.30000/task
XANADU	Photonic	N/A
IONQ	Trapped-ion	$0.03000/shot + $0.30000/task
QUANTINUUM	Trapped-ion	N/A

QMLaaS Overview

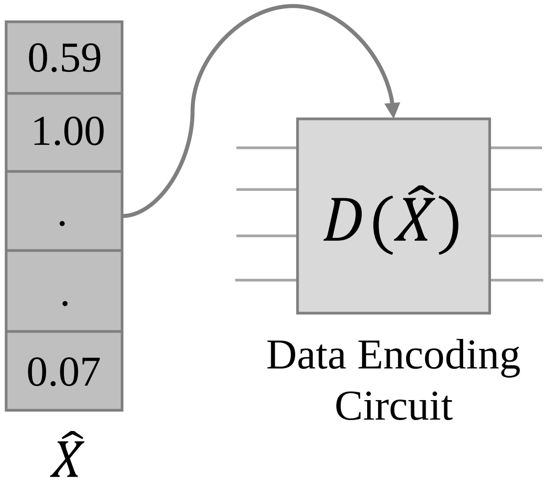


(Step-1) Data Pre-Processing

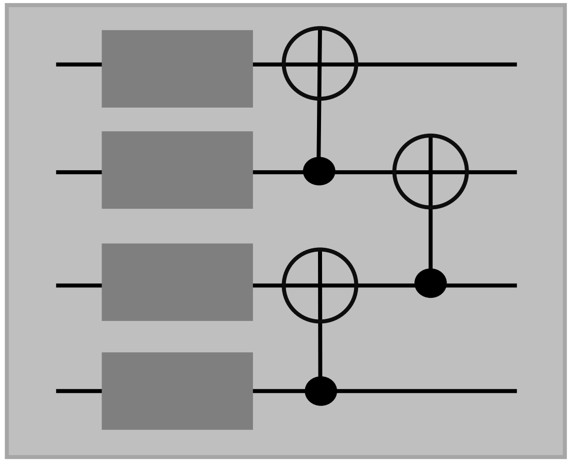
- NISQ devices struggle with large images: limited qubits, high error rates and complex data encoding.
- Dimensionality Reduction: reduce input data size.
  - PCA, LDA, Autoencoders, Resize, etc.
- Normalization: to prevent feature overlap in quantum encoding.
  - Min-max, max-absolute, etc.



(Step-2) Design and Encode



Parameterized Quantum Circuit

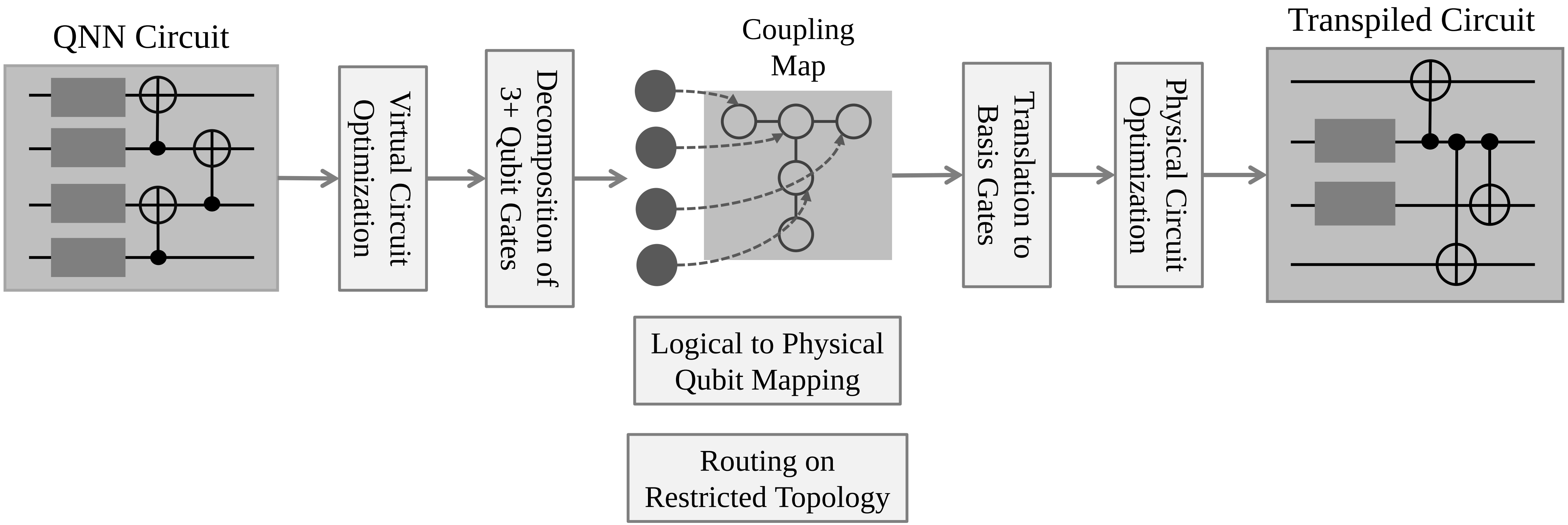


Basis Encoding
Amplitude Encoding
Angle Encoding
Quantum Circuit Search (QCS)
…

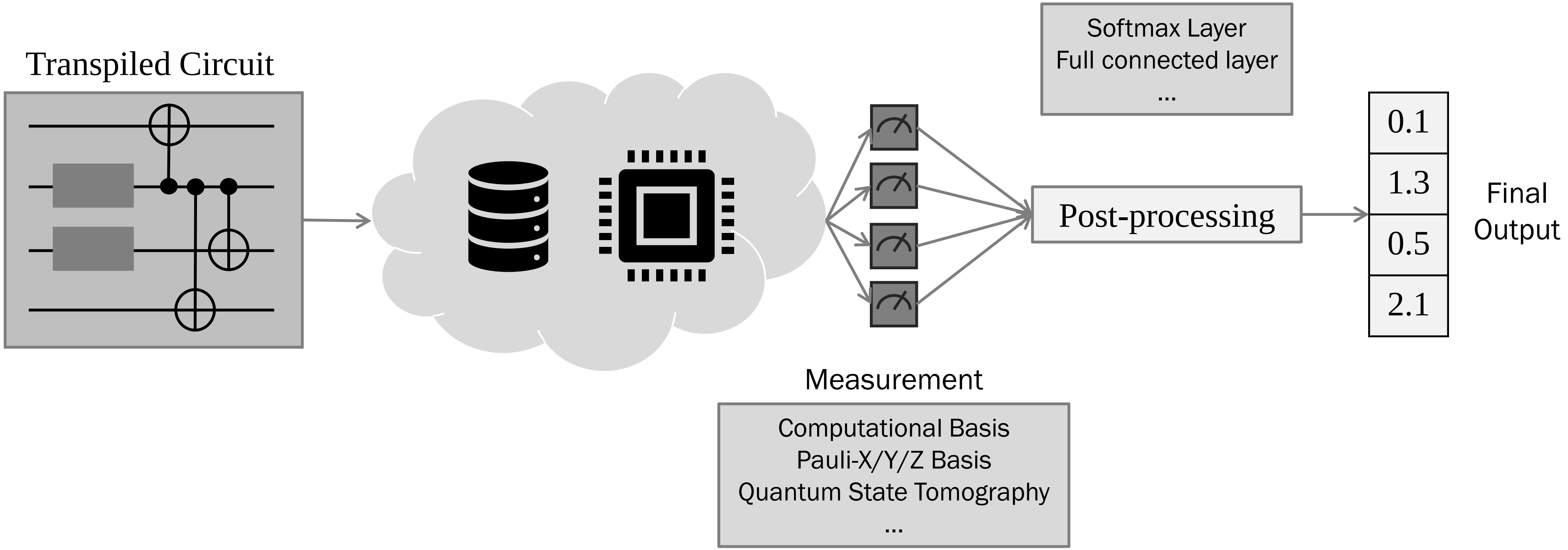
Circuit-1 to 18 [1]
Random Search
Evolutionary Search
RL-based Search
…

[1] Sukin Sim et al. "Expressibility and entangling capability of parameterized quantum circuits for hybrid quantum-classical algorithms." *Advanced Quantum Technologies* 2, no. 12 (2019)

(Step-3) Transpile and Map



(Step-4) Execute and Measure



(Step-5 & 6) Gradient Calculation & Optimization

Backpropagation not feasible: **No-cloning Theorem.**

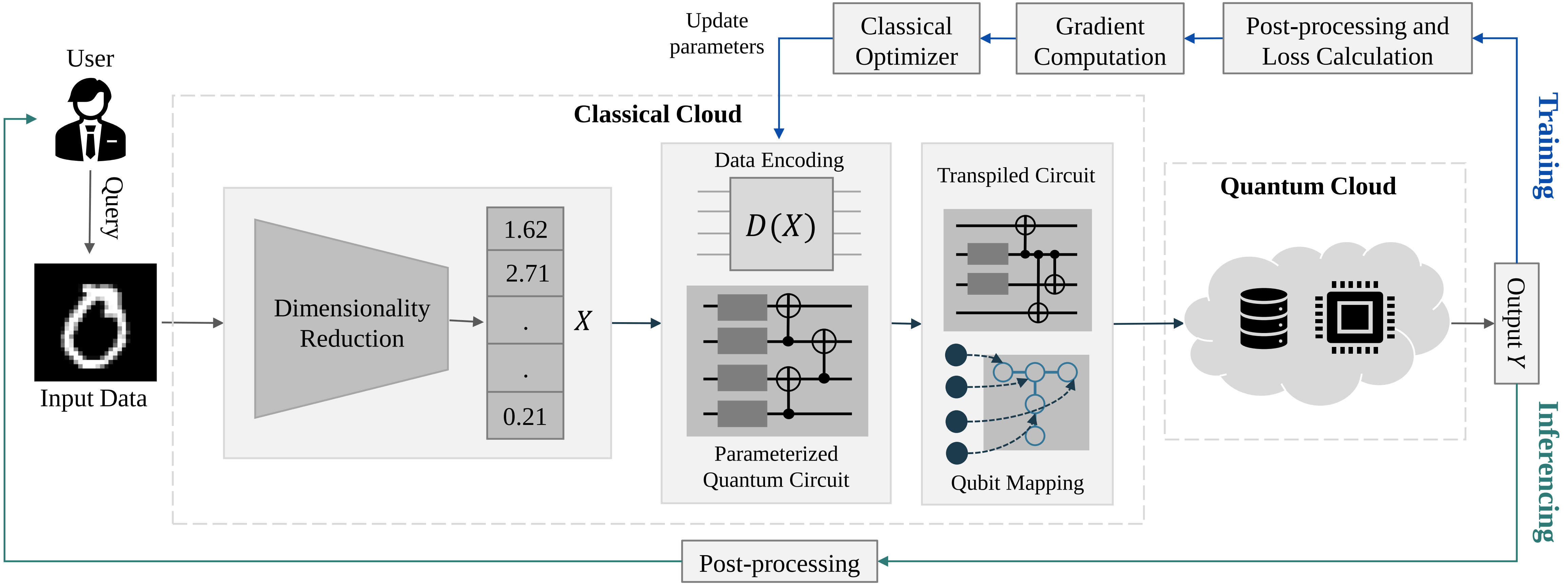
Alternate option?

Parameter-shift rule: $2n$ execution to calculate gradients n parameters. *(Accurate but Costly)*

Simultaneous Perturbation Stochastic Approximation (SPSA): 2 execution to estimate gradients of n parameters. *(Noisy but Efficient)*

Parameter Optimization? → Adam, Adagrad, SGD, etc. → Update QNN Parameters.

QMLaaS Pipeline



Why is QMLaaS at risk?

Interdependence on both classical and quantum resources.

Training QML Models is Expensive.

High Training Cost
QPUs are *2300X* more expensive compared to GPUs.

High Training Time
Toy QNNs can take days to train on real hardware (long queues).

Assets in QMLaaS

Training/Testing Data
Highly sensitive & expensive to acquire and process.

Data Encoding Circuit
Extensive evaluation, novel technique, encodes sensitive data.

PQC Architecture
Trained parameters, designing PQC is time consuming, IP.

Threats to Confidentiality

Classical Cloud

Threat?

Data Theft Attacks

When?

Raw Data → Data Pre-processing

Normalized Features → Encode & Design

Measured Data → Post-processing

Post-processing → User

Quantum Cloud

Threats?

Data Theft Attacks

QML IPs (encoding circuit, PQC)

Side-Channel Attacks

Model Stealing Attacks

When?

Transpiled Circuit → Quantum Hardware

Threats to Integrity

Classical Cloud

Threat?

Data Poisoning Attacks

When?

Raw Data → Data Pre-processing

Normalized Features → Encode & Design

Measured Data → Post-processing

Quantum Cloud

Threats?

Circuit Obfuscation Attacks

Fault Injection Attacks

Side-Channel Attacks

Low-quality Hardware Allocation

When?

Transpiled Circuit → Quantum Hardware

Threats to Availability

Classical Cloud

Threat?

Denial-of-Service Attacks

Latency Injection Attacks

When?

Normalized Features → Encode & Design

Post-processing → User

Quantum Cloud

Threats?

Denial-of-Service Attacks

Rerouting Attacks

Resource Exhaustion Attacks

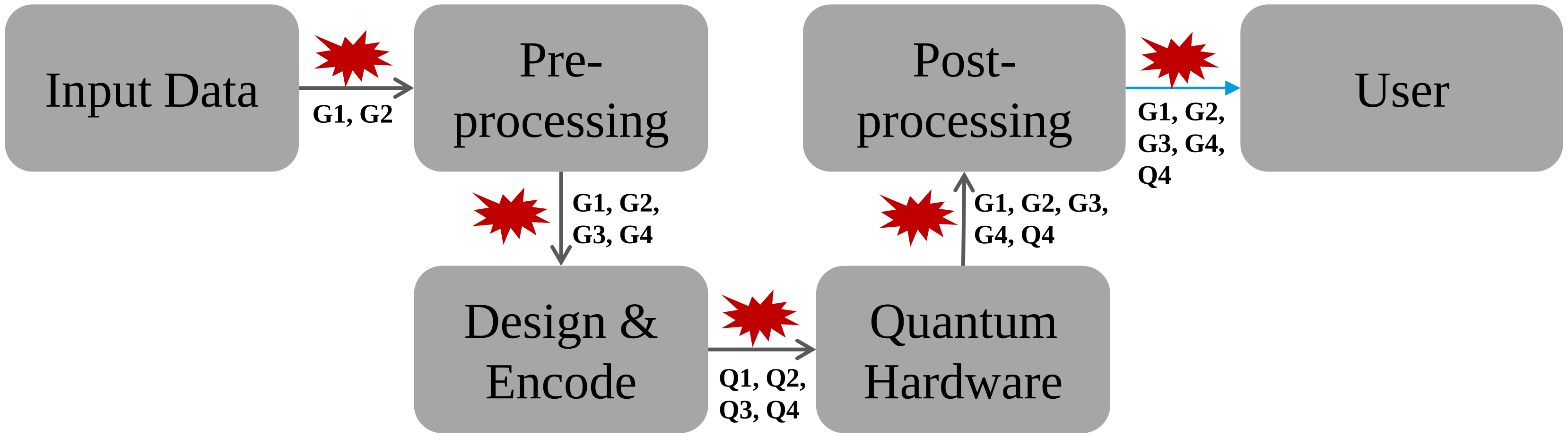
When?

Measured Data → Post-processing

Threats in QMLaaS Pipeline

Generic Threats (G)
1. Data/Output Theft (C)
2. Data/Output Poisoning (I)
3. Denial-of-Service (A)
4. Ransomware Attacks (A)

Quantum Threats (Q)
1. QML IPs (C)
2. Circuit Obfuscation (I).
3. Rerouting Attacks (I, A).
4. Latency Injection (A).



Conclusion

- QMLaaS (Quantum Machine Learning as a Service) is a promising hybrid model combining classical and quantum resources.
- Our work provides a comprehensive overview of each QMLaaS framework component.
- We identify critical security concerns specific to the hybrid QMLaaS architecture.
- Addressing these security challenges is essential for secure, reliable QMLaaS deployment.