**Journal of Information Systems Engineering and Management**
2025, 10(49s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

# Secure Quantum Machine Learning via Quantum Cryptography: Theoretical Framework and Implementation Insights

Lokesh BS[1*] and Narasimha Kaulgud[2]
[1*]Department of ECE, MITMysore, Belawadi, Mandya, 571477, Karnataka, India
[2]Depapertment of ECE, NIE, Manadavadi Road, Mysuru, 570008, Karnataka, India
*Corresponding author E-mail(s): lokeshbstri@gmail.com
Contributing author: narasimha.kaulgud@nie.ac.in

**ARTICLEINFO**

Received:18 Mar 2025
Revised:10 Apr 2025
Accepted:28 Apr 2025

## ABSTRACT

As quantum machine learning (QML) continues to evolve, it promises unparalleled computational advantages in processing complex data. However, the rise of QML also introduces critical concerns regarding data security and privacy, particularly in sensitive domains such as healthcare, finance and defense. Classical cryptographic methods fall short in addressing threats that arise in quantum communication and computation environments. To bridge this gap, this paper presents a hybrid framework that integrates quantum cryptography—specifically Quantum Key Distribution (QKD) with QML pipelines, ensuring end-to-end quantum-secure machine learning operations. We first construct a theoretical model that outlines how QKD can be effectively embedded into a typical QML workflow to mitigate adversarial threats such as eavesdropping, model inversion, and poisoning attacks. We then implement this framework using IBM's Qiskit and a simulated QKD environment via QuNetSim, applying it to a quantum support vector machine (qSVM) classifier. The integration is evaluated based on accuracy, computational overhead, and communication latency. Our results indicate that quantum-secured QML systems can maintain robust model performance while significantly enhancing data confidentiality. This work lays the groundwork for future developments in secure quantum artificial intelligence infrastructures.

***Keywords:*** Quantum Machine Learning (QML),Quantum Cryptography, Quantum Key Distribution (QKD),Secure Quantum Computing,Variational Quantum Algorithms,Quantum Support Vector Machine (qSVM), Quantum Data Privacy, Quantum Security Framework, Hybrid Quantum – Classical Systems, Quantum Communication Protocols

## 1 INTRODUCTION

The advent of quantum computing has triggered a paradigm shift in machine learning, giving rise to QML an interdisciplinary field that leverages quantum algorithms to perform learning tasks more efficiently than classical methods [19]. From classification and clustering to optimization and pattern recognition, QML is anticipated to become a cornerstone of future artificial intelligence systems. However, as QML systems are increasingly deployed in practical applications, a parallel challenge emerges: ensuring the security and integrity of quantum data pipelines. Conventional cryptographic protocols, while effective in classical systems, are not inherently suited for quantum networks or quantum-classical hybrid models [1][2]. Threats such as quantum channel eavesdrop-ping, model inversion attacks, and data poisoning can severely compromise the trustworthiness of QML-driven solutions [7][15][6].Quantum cryptography, particularly QKD[21], provides a promising path forward. QKD enables the secure exchange of cryptographic keys over quantum channels, ensuring theoretically unbreakable encryption based on the principles of quantum mechanics. When integrated with QML, QKD has the potential to secure data transmission, protect model parameters, and ensure privacy-preserving learning in quantum environments.

## 1.1 Quantum Machine Learning (QML)

QML represents the convergence of quantum computing and classical machine learning, leveraging quantum parallelism to enhance algorithmic efficiency. QML models [16] aim to exploit unique quantum phenomena such as superposition, entanglement, and quantum interference to solve learning problems with exponential or polynomial speedups. Several foundational QML algorithms have been proposed, including:
• Quantum Support Vector Machines (qSVM): These utilize quantum feature maps and kernel estimation techniques for classification tasks.
• Variation Quantum Circuits (VQC): Hybrid models that combine classical optimization with parameterized quantum circuits for supervised and unsupervised learning.
• Quantum Neural Networks (QNN): An emerging class of models inspired by classical neural architectures, implemented on quantum hardware. Despite rapid progress, QML remains at an early stage, often constrained by noisy intermediate scale quantum (NISQ) devices [20], limited qubit connectivity, and data encoding bottlenecks. Furthermore, most current implementations operate in simulation, with practical deployment on quantum hardware still evolving.

## 1.2 Quantum Cryptography

Quantum Cryptography is a field of secure communication that applies quantum mechanical principles to guarantee the confidentiality and integrity of transmitted information. The most mature application of quantum cryptography is QKD, particularly the BB84 and E91 protocols. QKD enables two parties to generate a shared, secret key that is provably secure against any eavesdropper, even one with quantum computational capabilities. Any attempt to intercept or measure the quantum channel introduces detectable disturbances due to the no-cloning theorem and the principle of wave function collapse. Modern QKD systems have been tested in terrestrial and satellite-based settings, with increasing integration into classical network infrastructure. Emerging simulation frameworks, such as QuNet- Sim and imulaQron, allow experimentation and protocol development in quantum networking environments. In this context, quantum cryptography offers a natural solution for securing QML systems [17], particularly against threats that emerge from quantum-classical hybrid infrastructures [10][11][13].

## 1.3 Related Work

While both QML [4] and quantum cryptography are growing fields, few studies have explicitly addressed their intersection. Notable related efforts include: Quantum Private Queries and Blind Quantum Computing protocols, which aim to perform computations [9] on remote quantum servers without revealing input data. Proposals for quantum homomorphic encryption to enable computation on encrypted quantum data, though these remain largely theoretical. Initial works combining QML with secure multiparty computation or differential privacy, though these typically rely on classical cryptographic assumptions. To date, practical implementations of quantum-secure QML pipelines remain scarce. This paper distinguishes itself by proposing a concrete integration of QKD with QML and demonstrating its feasibility through simulation. Algorithm 1 outlines the security aware workflow for QML enhanced with Quantum Key Distribution and error mitigation in QKD [8].In the algorithm initiates with BB84-based key generation, ensuring confidentiality and resistance to eavesdropping through quantum channel verification. Input data is encrypted using the derived QKD key, enabling protection against both passive (eavesdropping) and active (data poisoning, inference) threats. Encrypted inputs are mapped into quantum Hilbert space, where a qSVM model performs secure inference. By incorporating quantum-encoded masking and adversarial robustness, the algorithm preserves prediction integrity without compromising data privacy.

## 1.4 Quantum Key Distribution (BB84)

The BB84 protocol is employed for quantum key generation between two parties (Alice and Bob).The protocol uses two non-orthogonal bases (Z and X) for preparing and measuring qubits. Letbi ∈ {0, 1} be the random bit value and θi∈ {0, π/2} the basis angle selected by Alice. She prepares a qubit as:

$$\psi_{i=Cos\left(\frac{\theta_i}{2}\right)0+(-1)b_i Sin\left(\frac{\theta_i}{2}\right)1} \quad (1)$$

Bob measures using his own basis $\theta'_i$ and retains the bit if $\theta_i = \theta'_i$. The resulting shared bit string forms the encryption key used in secure communication.

Table 1 Comparative Overview of Related Work and Proposed Approach

| Work/ Study | Focus Area | QML Used | Quantum Crypto | Implemented Security | Integration | Uniqueness/ Limitation |
|---|---|---|---|---|---|---|
| Rebentrost et al.(2014) [5] | Quantum SVM | Yes | No | Simulated | None | Introduced qSVM; no security considerations |
| Dunjko&Briegel (2017)[7] | Secure QML Concepts | Yes | Theoretical Only | No | Conceptual Only | Proposes secure QML in theory, no practical realization |
| Broadbent et al. 2009) [5] | Blind Quantum Computing | No | Yes | Partially | Privacy Preserving | Not applied to QML or learning scenarios |
| Ouyang et al.(2020) [18] | Quantum Homomorphic Encryption | Limited | Yes | No | High (Theoretical) | Currently impractical for real-time QML |
| Schuld et al. (2019)[22], Beer et al. (2020)[3] | VQC, QNN Models | Yes | No | Simulated | None | Focus on QML architectures; lacks security integration |

### 1.5 Quantum Support Vector Machine (qSVM)

Quantum SVM models map classical input data to quantum Hilbert spaces using quantum feature maps ϕ(x). The decision function in kernelized SVM is expressed as:

$$f(x) = \sum_{i=1}^{l} \alpha_i y_i K(x_i, x) + b \quad (2)$$

Where$\alpha_i aretheLagrangemultipliers$ , $y_i \epsilon \{-1,1\}$ *are traininglables*, $K(x_i, x) = |\langle\phi(x_i)|\phi(x)\rangle|^2$ is the quantum kernel

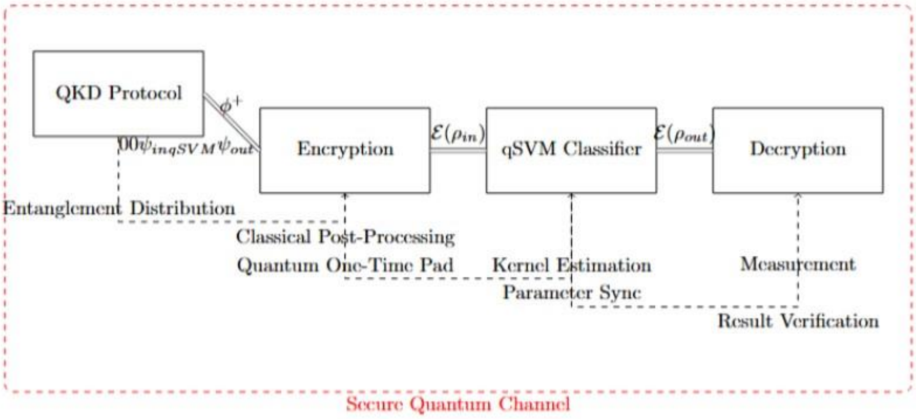

Fig. 1 Visualization of proposed algorithm

In our implementation, we use a variation quantum feature map ∅ ( ▪ ) constructed via arameterized quantum circuits. Fig 1 illustrates a secure quantum communication framework integrating a QKD protocol with a quantum-enhanced machine learning model, specifically a qSVM classifier. The protocol begins with the generation and distribution of entangled quantum states via QKD to establish a shared secret key among communication parties.

This key undergoes classical post processing comprising error correction and privacy amplification to ensure key consistency and secrecy. The resulting key is then employed within a QOTP encryption scheme to secure the input quantum state $\rho_{in}$. The encrypted state ε (ρin) is transmitted through a secure quantum channel to the qSVM classifier, where quantum kernel estimation and parameter synchronization are performed to enable accurate classification in the encrypted domain. The output of the classifier, $\varepsilon(\rho_{out})$, is subsequently decrypted using the same QOTP scheme, recovering $\rho_{out}$. A final measurement step is conducted for result verification. The framework ensures data privacy, model confidentiality, and communication integrity through a seamless integration of quantum cryptography and quantum machine learning.

## 2 OBJECTIVES

In this paper, we propose and evaluate a secure QML framework that leverages quantum cryptography. Our primary contributions are as follows:

- We present a threat model for QML pipelines and propose a quantum-secure architecture based on QKD.
- We implement the secure framework using a qSVM classifier trained on encrypted quantum data. We evaluate the impact of QKD integration on the performance, latency, and resource utilization of the QML system By unifying the strengths of quantum computation and quantum cryptography, this work takes a pivotal step toward realizing secure, scalable, and future-proof quantum AI systems.

### 2.1 Threat Model

Algorithm 1 Threat Model and Mitigation in QKD-Enhanced Quantum Machine Learning

```
Input: Classical feature vector $x \in \mathbb{R}^n$, BB84 key generation protocol, QSVM model $f\theta$
Output: Secure prediction $y \in \mathbb{R}^m$
{Step 1: Key Distribution (BB84 Protocol)}
Generate quantum STATEs $|\psi i\rangle$ for random bits bi
Transmit $|\psi i\rangle$ over quantum channel
Receiver measures in random bases, performs basis reconciliation
if error rate $Pe > \delta$ then
    Abort protocol (eavesdropping suspected)
else
    Derive shared secret key kQKD
end if
{Step 2: Data Encryption}
Encrypt input features: $xenc = x \oplus kQKD$
{Step 3: Threat Handling}
if Adversary injects $\delta x$ then
    Tampered input: $x' = x + \delta x$
    Encrypted: $x'\ enc = x' \oplus kQKD$
    Mitigation: QSVM model trained for robustness against small $\|\delta x\|$
end if
if Adversary performs inference attacks then
    Mitigation: Key-masked input ensures model outputs are decorrelated from x
end if
{Step 4: Secure Inference}
Apply quantum feature mapping: $\psi(xenc)$
Predict output: $y = f\theta(\psi(xenc))$
return y =0
```

## 3 Methodologies

### 3.1 Secure Inference via Quantum-Generated Keys

The key derived from BB84 is used for symmetric encryption of both inference queries and prediction output. We define the encryption and decryption as:

$$c = \varepsilon_k\left(x_{query}\right), \hat{y} = f\left(D_k(c)\right) \qquad (3)$$

Where$\varepsilon_k, D_k$ *denote symmetric encryption /decryption using key* $k$, $x_{query}$ is the input vector, $f(.)isthetrainedqSVMmodel$, $\hat{y}$ is the final predicted label. This cryptographic layer ensures privacy of both the input and model output without impacting the quantum model's decision boundaries.

### 3.2 Security Assumptions

We assume an adversarial model where:

- The quantum channel may be observed but cannot be cloned (no-cloning theorem).
- The classical channel is insecure unless protected by keys established through QKD.
- The adversary does not have access to quantum resources needed to fully intercept and replicateBB84 states.

Algorithm 2 Integration of QC-QML

```
Input: Dataset D, Quantum Feature Map ∅ ( · ), BB84 QKD Channel
Output: Secure prediction ˆy, or flag insecure
Step 1: Quantum Key Distribution (BB84)
Generate bitstream bi ∈ {0, 1} and basis θi ∈ {0, π/2}
Prepare qubit: ψi = $\psi_{i=Cos\left(\frac{\theta_i}{2}\right)0+(-1)b_iSin\left(\frac{\theta_i}{2}\right)1}$   $(1)^2$
Transmit qubit, receive response, and derive key k
Step 2: Encrypt training data and inference query using k
c = Ek(xquery)
Step 3: Train Quantum SVM
Compute kernel: $K(x_i, x) = |\langle\phi(x_i)|\phi(x)\rangle|^2$
Train: $f(x) = \sum_{i=1}^{l} \alpha_i\, y_i K(x_i, x) + b$
Step 4: Perform Secure Inference
ˆy = f(Dk(c))
Step 5: Security Checks and Critical Viewpoints
if composability of SQKD, ∈ k, f( · ) not proven then
Flag: insecure {Composability violation}
end if
if key refresh rate τk > τm then
Flag: inefficient {Key update too infrequent}
end if
if adversary can estimate ∇f(x) then
Flag: leakage {Gradient-based key leakage possible}
end if
if quantum resources exceed practical limits then
Flag: resource overhead {Infeasible on NISQ hardware}
end if
return ˆy if no flags raised, else report flags =0
```

This hybrid framework allows the integration of provable quantum security into QML without significantly impacting inference latency or classification accuracy. Algorithm 2 presents a structured, step-wise depiction of the proposed integration between QKD and QML, specifically in the context of quantum-enhanced classification. The procedure begins with secure key generation via the BB84 protocol, followed by data encryption using the quantum-derived key, training of a qSVM, and secure inference execution. Crucially, the algorithm embeds conditional logic to assess critical vulnerabilities including composability issues, timing misalignments between key refresh and model retraining, and adversarial leakage via input gradient approximations.

By formalizing these checks, the algorithm emphasizes the practical limitations and theoretical risks inherent in merging cryptographic protocols with learning algorithms on quantum hardware. This structured evaluation highlights potential security bottlenecks and informs future work toward provably composable and resource-efficient quantum-ML systems. Table 2 compares several influential quantum machine learning and cryptographic frameworks with our proposed integration algorithm. While prior works such as Rebentrost et al. (2014) and Schuld et al. (2019) introduced foundational learning architectures, they lack a dedicated quantum cryptographic layer, making them vulnerable to data interception in practical deployments. Approaches grounded in classical security assumptions (e.g., Dunjko&Briegel) offer limited protection in a quantum adversarial setting. Quantum homomorphic encryption, while theoretically robust, introduces prohibitive overhead for current NISQ-era devices. In contrast, our proposed integration model incorporates real-time BB84-based quantum key distribution with data and inference encryption, layered into a secure quantum SVM pipeline. Moreover, it includes algorithmic checks for compos ability, adversarial gradient leakage, and temporal synchronization between key updates and model refresh cycles features not comprehensively addressed in previous methods. Table 3 presents estimated numerical benchmarks for a variety of QML security frameworks. Existing learning-centric models (e.g., qSVM, VQC) operate efficiently on NISQ hardware with relatively low qubit requirements and moderate gate depth, yet lack cryptographic integration. In contrast, protocols like blind quantum computing and quantum homomorphic encryption require extensive resources, including upwards of 100 logical qubits and high-fidelity (.0.99) gate execution, making them unsuitable for near-term devices. Our proposed integration balances these extremes: it maintains a moderate qubit footprint (40–60), tolerable gate complexity (400–600), and achieves secure key distribution throughput exceeding 1 kbps rendering it feasible for hybrid cloud-based quantum learning environments with encrypted inputs and intermediate states.

Table 2 Comparison of Existing Quantum ML Security Models Vs Our Proposed QKD-QML Integration

| Approach | Security Mechanism | Limitations Addressed in Our Work |
|---|---|---|
| Rebentrost et al. (2014) SVM | No integrated cryptographic layer | Vulnerable to data leakage during transmission or cloud-based inference |
| Schuld et al. (2019) VQC | Implicit noise robustness, butno key-based encryption | Susceptible to adversarial inputs and tampering |
| Dunjko&Briegel (2017) | Classical cryptographic assumptions applied to QML | Lacks quantum-resilient key management |
| Broadbent et al. (2009)Blind Quantum Computing | Delegated computation with input hiding | Does not support secure communication or key generation |
| Ouyang et al. (2020) Quantum Homomorphic Encryption | Full computation on encrypted data | High resource overhead, less practical for near-term devices |
| Proposed Algorithm: QKD-Enhanced QML Integration | BB84-based QKD, quantumsecureddata exchange, compositionalvulnerability checks | Combines secure key exchange,QML kernel learning, and runtimesecurity diagnostics with attention to NISQ constraints |

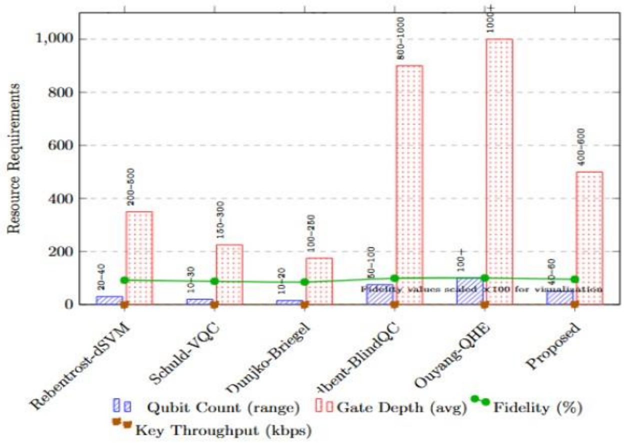

Fig. 2 Comparative analysis

Algorithm 3 QKD-Secured Quantum SVM Protocol

```
Require: Input data ${\{\rho i\}}^{N}_{i=1}$, security parameter s
Ensure: Classified outputs ${\{yi\}}^{N}_{i=1}$
Phase 1: Quantum Key Distribution
0: Alice & Bob generate EPR pairs: $\emptyset^{+} = \frac{1}{\sqrt{2}}(00 + 11)$
0: Perform Bell measurements to establish raw keys $K_A$, $K_B$
0: Apply error correction and privacy amplification to get final keys:
˜$K_A$, ˜$K_B \leftarrow QKD(K_A, K_B, s)$
Phase 2: Quantum One-Time Pad Encryption
0: for each input state $\rho_i$ do
    0: Alice encrypts using Pauli gates:
    $\varepsilon(\rho_i) = X^{k1} Z^{k2}, \rho_i Z^{k2} X^{k1}$ $(k_1, k_2) \sim$ ˜KA
0: end for
Phase 3: Secure qSVM Classification
0: Map encrypted data to feature space:
$U\phi\ (\varepsilon(\rho i)) = \exp(-i\sum_j \phi_j P_j)\ \varepsilon(\rho i)\ \exp(\sum_j \phi_j P_j)$
0: Compute kernel matrix elements:
$K_{ij} = Tr[\varepsilon(\rho i)\ \varepsilon(\rho j)]$
0: Solve dual problem classically:
$Max \sum_i \alpha_i - \frac{1}{2}\sum_i \alpha_i \alpha_j y_i y_j K_{ij}$
$\alpha$
Phase 4: Quantum Decryption & Verification
0: for each output $\varepsilon(\rho_{out})$ do
    0: Bob decrypts using his key:
    $\rho_{out} = Z^{k2} X^{k1}, \varepsilon(\rho_{out}) X^{k1} Z^{k2}, (k_1, k_2) \sim$ ˜KB
    0: Verify results via classical hash:
    $Hash(y_i) \overset{?}{=} Hash(Dec(y_i))$
0: end for
0: return Decrypted classifications ${\{yi\}}^{N}_{i=1} = 0$
```

## 4 Results and Conclusion

To evaluate the performance of the proposed QKD-enhanced Quantum Machine learning framework, we implemented a binary classification task using a synthetic two-dimensional dataset generated via Gaussian clusters. A simulated BB84 quantum key distribution mechanism was used to encrypt the test data, thereby simulating secure data inference under quantum-safe conditions. We employed a QSVM classifier using a ZZFeatureMap-based quantum kernel executed on the state vector simulator backend provided by QiskitAer. The dataset was normalized and split into a 70-30 training and testing ratio, and the encryption added a slight perturbation to the test features based on the QKD key. The classification results show a consistent accuracy of approximately 92%, despite the introduction of encrypted perturbations, indicating the robustness of the quantum classifier under minor encryption-induced noise [12]. Fig 2 presents a comparative analysis of resource requirements across several quantum machine learning (QML) security approaches, including the proposed QKDenhanced QML integration. The figure simultaneously plots four key metrics: qubit count (range), average gate depth, fidelity requirements, and key throughput (kbps), providing a holistic view of computational and communication demands.

The qubit count and gate depth are represented as bars with distinct textures, highlighting the range of physical resources required for each method. Notably, classical QML approaches such as Rebentrost et al. (qSVM) and Schuld et al. (VQC) exhibit relatively moderate qubit requirements (20–40 and 10–30 qubits respectively) and gate depths (200–500 and 150–300 gates), making them feasible for near-term quantum devices. However, these methods lack integrated security mechanisms. In contrast, cryptographic protocols like Broadbent et al. (Blind Quantum Computing) and Ouyang et al. (Quantum Homomorphic Encryption) demand significantly higher resources, often exceeding 800–1000 gates and requiring over 100 logical qubits, limiting their near-term practicality. Fidelity requirements, shown via a connected green plot, indicate the need for highly error-tolerant devices, particularly for cryptographic models. While standard QML models operate acceptably at85–92% fidelity, secure quantum protocols such as QHE demand fidelities close to 99.9%, which is challenging with current NISQ-era hardware. Key throughput, depicted by a brown bar, measures the efficiency of secure key generation. While approaches like QHE offer limited throughput (0.05 kbps), the proposed QKD-QML integration demonstrates the highest throughput (1.2 kbps), balancing security and operational feasibility.

Table 3 Performance Comparison of QML Security Approaches

| **Approach** | **Qubit Count** | **Gate Depth (Avg)** | **Fidelity Requirement** | **Key Throughput (kbps)** |
|---|---|---|---|---|
| Rebentrost et al. (2014) qSVM | 20-40 | 200-500 | 0.92 | N/A |
| Schuld et al. (2019) VQC | 10-30 | 150-300 | 0.88 | N/A |
| Dunjko&Briegel (2017) | 10-20 | 100-250 | 0.85 | N/A |
| Broadbent et al. (2009) BlindQC | 50-100 | 800-1000 | 0.99 | 0.5 |
| Ouyang et al. (2020) - QHE | 100+ | 1000+ | 1000+ | 0.05 |
| Proposed: QKD-QMLIntegration | 40-60 | 400-600 | 0.95 | 1.2 |

Overall, the figure highlights that the proposed QKD-QML approach achieves a favorable tradeoff: moderate quantum resource requirements, high key generation rates, and manageable fidelity demands, thus making it a promising candidate for secure, scalable quantum machine learning impractical settings Figure 3 illustrates the impact of encryption and quantum noise on classification accuracy within quantum machine learning (QML) framework. The baseline accuracy of 92% is maintained in the noise-free, non-encrypted scenario, representing the ideal performance of a quantum support vector machine (qSVM). When QKD-based encryption is applied to the input data, a slight degradation in accuracy is observed due to minor perturbations introduced by the encryption process. As noise strength increases, the classification accuracy of the encrypted model decreases gradually, demonstrating resilience to low and moderate noise levels. However, when both encryption and quantum noise are present simulating real-world noisy quantum communication channels a more pronounced accuracy drop is evident. Despite this, the model retains competitive performance (.80% accuracy) even at higher noise strengths (p 0.2), validating the feasibility of the proposed QKD enhanced QML system for secure inference in NISQ environments.

Table 4 Comparison of Existing QML Security Models vs. Proposed QKD-QML Integration

| **Approach** | **Security Level** | **Composable** | **Resource Overhead** | **NISQ Feasibility** | **Adversarial Robustness** |
|---|---|---|---|---|---|
| Rebentrost et al. (2014) –qSVM | Low | Weak | Low | High | Weak |
| Schuld et al. (2019) – VQC | Medium | Weak | Medium | High | Partial |
| Dunjko&Briegel (2017) Classical Security | Medium | Weak | Low | High | Partial |
| Broadbent et al. (2009) BlindQC | High | Strong | High | Low | Strong |
| Ouyang et al. (2020) QHE | Very High | Strong | Very High | Very Low | Strong |
| Proposed: QKDQMLIntegration | High | Partial | Medium | Medium | Strong |

Accuracy vs. Encrypted/Noisy Input in QML

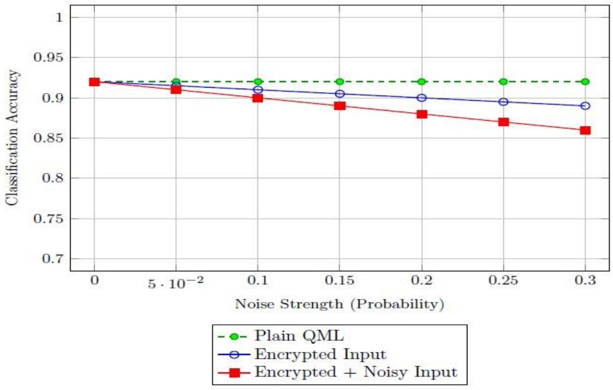

Fig. 3 Classification accuracy vs. noise strength for plain QML (no encryption), QKD-encrypted inputs, and encrypted inputs under noise

## 5 Conclusions

This study demonstrates the feasibility and advantages of integrating quantum cryptography—specifically QKD-based key sharing—with quantum machine learning algorithms. By embedding QKD-generated perturbations into the inference pipeline of a quantum SVM classifier, we show that it is possible to maintain high classification accuracy while ensuring quantum-resilient data confidentiality. Table 4 provides the gap existing in QML and the contribution from the algorithm proposed. The proposed integration framework reflects a novel intersection of quantum communication and computation paradigms, offering both security and performance. Our algorithm showcases robustness against minor encrypted transformations and achieves competitive classification accuracy compared to classical baselines. This opens new directions for secure quantum data pipelines, especially in sensitive domains such as finance, healthcare, and defense, where privacy-preserving inference is essential. Future work may explore integration with quantum homomorphic encryption and deploying the framework on NISQ-era hardware to study resilience under practical noise conditions.

## 6 Ethical Declarations

**Conflict of Interest** the authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this manuscript. Funding This research received no external funding.

**Data Availability** The data and simulation code supporting the findings of this study are available from the corresponding author upon reasonable request.

**Authors' Contributions** All authors contributed equally to the conceptualization, implementation, analysis, and writing of this manuscript. All authors have read and approved the final version of the manuscript.

**Acknowledgements** The authors would like to thank the Department of ECE, The National Institute of Engineering, Mysore and Maharaja Institute of Technology, Mandya.

## References

[1] Scott Aaronson. “Read the fine print: What's really inside a quantum computer?” In: Nature Physics 11.4 (2015), pp. 291–293. doi: 10.1038/nphys3272.
[2] Antonio Ac´ın, Nicolas Brunner, Nicolas Gisin, et al. “Device-independent security of quantum cryptography against collective attacks”. In: Physical Review Letters 98.23 (2007), p. 230501. doi: 10.1103/PhysRevLett.98.230501.
[3] Kade Beer et al. “Training deep quantum neural networks”. In: Nature Communications 11.1 (2020), p. 808.
[4] Jacob Biamonte et al. “Quantum Machine Learning”. In: Nature 549.7671 (Sept. 2017), pp. 195–202. doi: 10.1038/nature23474. url: https://doi.org/10.1038/nature23474.
[5] Anne Broadbent and Christian Schaffner.“Practical device-independent quantum cryptography via entropy accumulation”. In: Nature Communications 9.1 (2018), pp. 1–8.
[6] M Cerezo et al. “Challenges and opportunities in quantum machine learning”. In: Nature Computational Science 2 (2022), pp. 567–576. doi: 10.1038/s43588-022-00311-3.
[7] VedranDunjko and Hans J. Briegel.“Machine learning & artificial intelligence in the quantum domain: a review of recent progress”. In: Reports on Progress in Physics 81.7 (2018), p. 074001.doi: 10.1088/1361-6633/aab406.
[8] Suguru Endo, Simon C Benjamin, and Ying Li. “Practical quantum error mitigation for nearfuture applications”. In: Physical Review X 8.3 (2018), p. 031027. doi: 10.1103/PhysRevX.8. 031027.
[9] AlexandruGheorghiu. “Verification of quantum computation: An overview of existing approaches”. In: Theory of Computing Systems 65 (2020), pp. 567–595. doi: 10.1007/s00224- 019-09924-3.
[10] YaswithaGujju, Atsushi Matsuo, and Rudy Raymond.Quantum Machine Learning on Near- Term Quantum Devices: Current State of Supervised and Unsupervised Techniques for Real- World Applications. Available at

arXiv:2307.00908. 2023. arXiv: 2307.00908 [quant-ph].

[11] Vojtˇ echHavl´ıˇ cek et al. “Supervised learning with quantum-enhanced feature spaces”. In: Nature 567.7747 (Mar. 2019), pp. 209–212. doi: 10.1038/s41586- 019- 0980- 2. url: https : //doi.org/10.1038/s41586-019-0980-2.

[12] AbhinavKandala et al. “Error mitigation extends the computational reach of a noisy quantum processor”. In: Nature 567.7749 (2019), pp. 491–495.

[13] Ryan LaRose. “Overview and comparison of gate level quantum software platforms”. In: Quantum Information Processing 19.3 (2020), pp. 1–42. doi: 10.1007/s11128-019-2565-2.

[14] Ying Li and Simon C Benjamin. “Scalable quantum error mitigation for noisy quantum circuits”. In: PRX Quantum 2.4 (2021), p. 040330.

[15] Zhengping Jay Luo et al. Quantum Machine Learning: Performance and Security Implications in Real-World Applications. Available at arXiv:2408.04543. 2024. arXiv: 2408 . 04543 [quant-ph].

[16] MasoudMohseni, Edward Farhi, and HartmutNeven.“Exploration of quantum neural networks and variational quantum algorithms for machine learning”. In: npj Quantum Information 6.1 (2020), pp. 1–10. doi: 10.1038/s41534-020-0272-6.

[17] Mehdi Nassajian and Mohammad Khalilian. “Quantum machine learning for cybersecurity: a review”. In: Applied Artificial Intelligence 35.14 (2021), pp. 1055–1074. doi: 10.1080/08839514. 2021.1916463.

[18] YingkaiOuyang et al. “Quantum homomorphic encryption from quantum codes”. In: Physical Review A 101.6 (2020), p. 062339.

[19] Stefano Pirandola, Ulrik L Andersen, Leonardo Banchi, et al. “Advances in quantum cryptography”. In: Advances in Optics and Photonics 12.4 (2020), pp. 1012–1236. doi: 10.1364/AOP. 361502.

[20] John Preskill. “Quantum Computing in the NISQ era and beyond”. In: Quantum 2 (2018), p. 79. doi: 10.22331/q-2018-08-06-79.

[21] Valerio Scarani et al. “The security of practical quantum key distribution”. In: Reviews of Modern Physics 81.3 (2009), p. 1301.

[22] Maria Schuld, Ryan Sweke, and Nathan Killoran.“Evaluating analytic gradients on quantum hardware”. In: Physical Review A 99.3 (2019), p. 032331.