International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2025.4.1

E-ISSN : 2454-6135

Volume. 11, No.4
April – 2025

Subject Review: AI-Driven Security in Quantum Machine Learning: Vulnerabilities, Threats, and Defenses

Farah Neamah Abbas[1], Mohanad Ridha Ghanim[*2], Rafal Naser Saleh[3]

Department of Computer Science

College of Education, Mustansiriyah University

Baghdad, Iraq

Iraq

ABSTRACT

Quantum Machine Learning (QML) has advanced significantly thanks to the combination of Quantum Computing (QC) with Artificial Intelligence (AI), hence releasing computational benefits over conventional methods. This synergy does, however, also bring fresh security flaws like adversarial attacks, quantum noise manipulation, and cryptographic weaknesses. This work offers a thorough investigation of QML security along with an examination of its special vulnerabilities resulting from hardware-induced faults, quantum variational circuits, and quantum data encoding. We methodically investigate adversarial attack techniques using the probabilistic character of quantum states including side-channel assaults, quantum noise injection, and algorithmic perturbations. We also assess innovative defensive strategies such differential privacy, quantum adversarial training, quantum error correction (QEC), cryptographic techniques include Quantum Homomorphic Encryption (QHE), We offer a hybrid AI-driven method for protecting QML models against developing threats by linking artificial intelligence and quantum security frameworks. This work emphasizes the importance of developing quantum-safe AI systems and consistent adversarial robustness standards. The results help to advance AI-enhanced quantum security, thereby guaranteeing the future of QML applications is efficient, strong, and resistant to adversarial attack.

Keywords: Adversarial Attacks in QML, Quantum Security Frameworks, Quantum Error Correction (QEC), Quantum Machine Learning (QML), Post-Quantum Cryptography (PQC), *Quantum Homomorphic Encryption* (QHE).

1. INTRODUCTION

Recent developments in quantum technology have advanced hardware engineering and algorithm development noticeably. By building their own technological stacks, some companies and nations are aggressively funding Quantum Computing (QC). Though large-scale, noise-resilient quantum computers have great promise to speed calculations across many domains [1, 2], such systems are not likely to be accessible right now. Thus, modern studies concentrate on using the features of noisy intermediate-scale quantum (NISQ) devices [3]. Among several disciplines, Machine Learning (ML) is generally agreed to be one of the first ones that will profit from NISQ devices [4, 5, 6]. Early studies in Quantum Machine Learning (QML) have produced new approaches like quantum clustering [4], quantum deep learning [7], and quantum reinforcement learning [8]. These advances imply that QML could increase performance in ML tasks and raise computing efficiency. But including QC also raises special security issues outside of conventional ML weaknesses [9]. Novel attack routes may be able to compromise quantum algorithms and hardware, hence specific security frameworks are needed to protect data and computational operations.

Research in QML therefore has to consider not just computing efficiency but also the security consequences of quantum-enhanced learning models.

With an eye toward both vulnerabilities and solutions, this overview of the literature addresses security issues related to Quantum Machine Learning (QML). The work closely examines security concerns unique to QML, including possible attack tactics using quantum data encoding or use of quantum noise and vulnerabilities in quantum classifiers running in high-dimensional environments. Given the complexity of QML and their potential real-world uses, these security issues are rather important as they underline the need of thorough verification methods to maintain both security and computational advantage. Additionally discussed in the book are many proactive protective techniques meant to reduce these hazards. Among these are adversarial training to boost model resilience against attacks, privacy-preserving methods to guard quantum data, stability and dependability of QML models, even hardware noise as a means of augmenting the resilience of quantum models rather than seeing it just as a constraint.

This survey gives academics and industry practitioners a better knowledge of the security scene in QML by means of a thorough evaluation of both the vulnerabilities and the related countermeasures. Development of increasingly safe and efficient quantum-based machine learning systems depends on this understanding, which guarantees that as quantum computing develops, its uses in ML stay both effective and robust against new challenges..

The paper is organized as follows: Section 2,3 provides an overview of the basic principles of QC and QML. Section 4 presents the approach used for this systematic survey. Section 5 delves into the unique challenges of QML models. Section 6 outlines potential defense mechanisms and the inherent resilience of these models. Finally, Section 7 offers guidance for practitioners by highlighting potential security gaps in QML that warrant future exploration.

2. QUANTUM COMPUTING

2.1 Brief History of Computation

Turing machines establish the boundaries of what is computable by means of stepwise algorithmic processes, so modern computational theory is mostly founded on them. Proposed by Alan Turing, the Universal Turing Machine (UTM) formalizes the theory that every algorithmic operation may be carried out on an adequately strong computing model. [10]

A. Computability and Complexity Classes

The Church-Turing thesis holds that a Turing-complete system can run any algorithmically computable function. Nonetheless, depending on the resources needed—time and space—computer issues are classified as either difficult or simple[11]:

- P (Polynom Time) problems solvable in polyn time—that is, those involving sorting, matrix multiplication..
- Problems for which a solution may be confirmed in polynomial time—that is, NP (nondeterministic poisson time—that is, Boolean satisfiability problem, Hamiltonian route).
- NP-Complete: At least as difficult as any other NP issue, this subset.
- Bounded-Error Quantum Polynomial Time: Issues easily solved by a quantum computer but may not be so easily solvable by a classical computer..

DOI : 10.31695/IJERAT.2025.4.1

When conventional methods are intractable—that is, when they call for exponential or super-polynomial time—quantum computing becomes indispensable. [12].

B. Classical vs. Quantum Computation

All classical computers employ the pragmatic implementation of a UTM called Von Neumann architecture. Quantum computers provide a different paradigm, however, using quantum parallelism to speed operations. [13].

Important quantum computing discoveries include of:

- **Shor's Algorithm (1994):**
  - ✓ Classical integer factorization (RSA breaking) is sub-exponential in complexity $O\ (2^{(n^{\frac{1}{3}}log^2 n)})$.
  - ✓ Shor's algorithm runs in polynomial time $O(n^3)$, leveraging quantum Fourier transforms for periodicity detection.
- **Grover's Algorithm (1996):**
  - ✓ Classical unsorted database search requires O(N) operations.
  - ✓ Grover's algorithm reduces this to $O(\sqrt{N})$ using quantum amplitude amplification.

These quantum speedups imply that in domains like cryptanalysis, optimization, and machine learning, quantum computing might surpass conventional computing [14].

2.2 Principles of Quantum Computing

While quantum bits (qubits) live in superposition, classical bits are binary—0 or 1:

$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$

where $\alpha, \beta \in C$ satisfy $|\alpha|^2+|\beta|^2=1$. A system with n qubits spans a Hilbert space of dimension 2^n, exponentially increasing its representational capacity [15].

2.2.1 Superposition and Quantum Parallelism

The Hadamard gate (H) creates superposition:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Thus, applying Hadamard gates to n qubits produces a uniform superposition of 2^n basis states, enabling quantum parallelism [16].

2.2.2 Entanglement and Nonlocal Correlations

Quantum entanglement occurs when the quantum state of one particle is correlated with another, irrespective of distance. For example, the Bell state [17]:

DOI : 10.31695/IJERAT.2025.4.1

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

measured in any basis ensures that both qubits collapse into the same state.

Entanglement enables:

- Quantum teleportation: sending qubit states without conventional information flow..
- Using one entangled qubit, superdense coding sends two classical bits of information.

2.2.3 Quantum Gates and Unitary Operations

Quantum computations are performed by applying unitary transformations [18]:

$U^{\dagger}U=I$

Examples:

- Pauli Gates:
  - $X|0\rangle=|1\rangle$, $X|1\rangle\ |0\rangle$ (NOT gate)
  - $Z|0\rangle=|0\rangle$, $Z|1\rangle=-|1\rangle$ (Phase flip)
- CNOT Gate (Entanglement Generator): $CNOT|00\rangle=|00\rangle$,$CNOT|10\rangle=|11\rangle$

Unitary evolution distinguishes quantum from classical probabilistic models by guarantees that information is never lost during computing [19].

2.2.4 Measurement and Wavefunction Collapse

Superposition of a qubit exists before measurement. Wavefunction collapse in measurement results from:

$P(0) = |\alpha|^2$,$P(1)=|\beta|^2$

Post-measurement, the system is irreversibly reduced to either $|0\rangle$ or $|1\rangle$, eliminating quantum superposition effects [20].

2.3 State-of-the-Art Quantum Computing

A. Current Hardware Limitations

Quantum hardware must achieve:

- Reducing decoherence resulting from environmental interactions results in high-fidelity qubit control [21].
- Fault tolerance: Quantum error correction requires logical qubits constructed from multiple noisy physical qubits [22].
- Current architectures:
- Superconducting Qubits (IBM, Google): Use Josephson junctions, requiring ultra-low temperatures (~15mK) [21].

DOI : 10.31695/IJERAT.2025.4.1

- Trapped Ions (IonQ, Honeywell): Leverage electromagnetic traps for stable long-lived qubits at room temperature [22].
- Photonic Qubits: Use quantum optics for non-interacting qubits, suitable for quantum communication [23].

B. Quantum Supremacy and NISQ Era

Quantum supremacy was demonstrated by Google's Sycamore (2019), which solved a random circuit sampling problem in 200s, infeasible for classical supercomputers [24]. However, current quantum computers operate in the Noisy Intermediate-Scale Quantum (NISQ) era, characterized by [25]:

- Limited qubit coherence times.
- High gate error rates.
- Absence of fault tolerance.

C. Future Directions: Fault-Tolerant Quantum Computing

The goal is to achieve error-corrected quantum computation [26]:

- Surface code error correction requires logical qubits constructed from ~1000 physical qubits.
- Topological quantum computing (Majorana fermions) aims to achieve hardware-level protection against errors.
- Near-term applications of NISQ devices include [27]:
- Variational Quantum Eigensolvers (VQE) for quantum chemistry.
- Quantum Approximate Optimization Algorithm (QAOA) for solving combinatorial problems.
- Quantum Machine Learning (QML) leveraging entanglement and Hilbert space representations.
- Quantum computing is not a replacement for classical computing but provides exponential speedups for specific problems. The key differences are [28]:
- Superposition & Entanglement enable massive parallelism.
- Unitary operations & measurement postulates define computation.
- Quantum speedup is problem-dependent, as only certain classes (e.g., factoring, search) benefit significantly.

Although ten years away are viable fault-tolerant quantum computers, research on NISQ algorithms, error correction, and hardware scaling is fast bringing the science towards usable quantum advantage [29].

3. QUANTUM MACHINE LEARNING

ML promises to be one of the earliest application fields to benefit from early adaptation of QC. Many approaches have already been proposed varying from operating on hard datasets consisting of quantum data, such as molecular states [30] and phases of matter [31], to quantum-inspired fully-classical approaches [32]. In this work, we concentrate on a particular subfield of QML that is sometimes referred to as *quantumassisted ML*. This subfield develops technique to *hybridize* classical ML with quantum algorithms.

DOI : 10.31695/IJERAT.2025.4.1

In this case, quantum algorithms are often represented as Parametrized Quantum Circuits (PQC) [33] that are parameterized by classical parameters, which can be tuned by classical methods during the training process. PCQs can be implemented as a stand-alone quantum model, or be a part for a hybrid quantum-classical architecture which is a preferred approach in the field for implementing more complex and bigger QML models [34].

3.1 Data encoding feature map

Fundamental in nature, quantum data encoding transfers conventional data into a Hilbert space of quantum states in Quantum Machine Learning (QML). Like kernel approaches in conventional machine learning, this metamorphosis serves as a feature map and directly affects quantum algorithm computing capacity [35]. We call the mapping procedure:

$$\Phi(x): x \in \mathbb{R}^{2N} \rightarrow |\psi(x)\rangle$$

where classical data x is transformed into a quantum state. The encoding strategies used in QML are crucial for efficiently leveraging quantum computing advantages. Two widely used methods are amplitude embedding and angle embedding [36].

A. Amplitude Embedding

Amplitude embedding is a logarithmically compact encoding method that maps a 2N-dimensional classical input vector into an N-qubit quantum state [37]. The encoded quantum state is given by:

$$|\psi(x)\rangle = \sum_i \psi_i(x_i)|i\rangle$$

where the coefficients $\psi_i(x_i)$ must satisfy the normalization constraint:

$$\sum_i |\psi_i(x_i)|^2 = 1$$

This encoding exploits the exponential state space of quantum systems, making it particularly suitable for high-dimensional data representations. It is often associated with a linear kernel in QML

B. Angle Embedding

Angle embedding utilizes quantum rotations to encode classical values into qubit phase angles [38]. This is expressed as:

$$\psi(x)\rangle = \otimes R_\theta(x_i)|0\rangle$$

where $R_\theta(x_i)$ represents a quantum rotation gate parameterized by the classical feature x_i. This method is hardware-efficient, resembling a cosine kernel, and is commonly used in variational quantum circuits for QML tasks.

3.2 Model Zoo

By use of Parameterized Quantum Circuits (PQC) for classification and other ML problems, Quantum Machine Learning (QML) enhances traditional machine learning (ML) approaches [39]. Following a hybrid quantum-classical method, a quantum binary classifier uses classical optimization techniques to modify the quantum circuit parameters while the quantum component (PQC) codes and analyzes input.

DOI : 10.31695/IJERAT.2025.4.1

3.2.1 Quantum Binary Classifiers

A quantum binary classifier consists of a PQC that can process either [40]:

- ❖ Quantum data: Directly obtained from quantum experiments or quantum feature maps.
- ❖ Classical data: Encoded into quantum states before processing.

The classification process involves:

1. Quantum State Preparation: Encoding classical features into quantum states using feature maps (e.g., amplitude or angle embedding).
2. Parameterized Quantum Circuit (PQC) Execution: A variational quantum circuit transforms the input quantum state.
3. Measurement:
    - ➢ A single-qubit measurement is performed to determine class probability.
    - ➢ Alternatively, multiple measurements compute the expectation value of an observable, which is then thresholded to classify the input.

The PQC parameters are optimized using classical gradient-based techniques (e.g., gradient descent with backpropagation) to minimize a loss function [41].

3.2.2 Quantum Neural Networks (QNNs)

Inspired by the success of neural networks (NNs) in conventional machine learning, quantum neural networks (QNNs) employ layer-wise quantum circuits as its computing units [42]. Although they use quantum unitary transformations rather than matrix multiplications, QNNs resemble feedforward neural networks (FNNs) and have been shown to have more expressivity than conventional NNs under some experimental settings.

Specialized QNN Architectures [43]:

1. Quantum Convolutional Neural Networks (Quanvolutional NNs)
    - ➢ Inspired by classical CNNs, these architectures leverage quantum feature maps to extract hierarchical representations from input data.
    - ➢ The convolutional layers use quantum gates instead of matrix multiplications.
2. Quantum Reinforcement Learning (QRL)
    - ➢ Extends classical reinforcement learning (RL) by leveraging quantum circuits for state updates.
    - ➢ Quantum policies can achieve advantages in exploration due to quantum superposition.
3. Quantum Generative Adversarial Networks (QGANs)
    - ➢ Extends classical GANs, where a quantum generator creates samples and a classical or quantum discriminator evaluates them.

DOI : 10.31695/IJERAT.2025.4.1

- Demonstrated applications in quantum chemistry and data synthesis.

4. Quantum Boltzmann Machines (QBMs)
   - Quantum analog of classical Boltzmann machines, used for unsupervised learning.
   - Encodes probability distributions using quantum Gibbs states.
5. Quantum Kernel Methods
   - Utilizes quantum feature maps to enhance the performance of support vector machines (SVMs) and Gaussian processes.
   - Provides exponential speedup for high-dimensional classification tasks.

Rapidly growing with fresh designs like Quantum Neural Networks (QNNs), Quantum Convolutional Network (QCNs), Quantum GANs (QGANs), and Quantum Kernel Methods is Quantum Machine Learning (QML). These models use quantum parallelism, entanglement, and interference to maybe surpass conventional ML in some fields. [44].

3.2.3 Hardware noise

Highly susceptible to hardware noise, quantum computing exposes inadvertent perturbations that compromise quantum states and cause computational mistakes [45]. Environmental interactions, quantum gate mistakes, manufacturing defects, and control faults cause these mistakes. Unlike conventional systems where mistakes can be fixed with redundancy, quantum systems suffer from decoherence and noise-induced state perturbations, so fault tolerance is a great difficulty [46].

1. Types of Quantum Noise and Adversarial Errors

Quantum noise can be categorized into different error channels, which are modeled using quantum operations (CPTP maps) [47]:

1.1 Bit-Flip and Phase-Flip Errors

These errors are equivalent to applying unwanted Pauli gates:

- Bit-flip (X) error: Flips the qubit state: $X|0\rangle=|1\rangle$, $X|1\rangle=|0\rangle$
- Phase-flip (Z) error: Inverts the relative phase: $Z|+\rangle=|-\rangle$, $Z|-\rangle=|+\rangle$

These are modeled as Pauli error channels:

$$\mathcal{E}(\rho) = (1-p)\rho + pX\rho X$$

for bit-flip errors with probability p.

1.2 Depolarization Noise

Depolarization transforms a qubit into a maximally mixed state, making all measurement outcomes equally probable [48]:

$$\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{2^n} I$$

where I is the identity matrix, and p is the depolarization probability.

DOI : 10.31695/IJERAT.2025.4.1

1.3 Decoherence and Loss of Quantum Interference

Decoherence results from unwanted coupling with the environment, leading to loss of superposition [49]:

T_1:Energy relaxation (spontaneous emission) T_2:Dephasing (loss of phase coherence)

These times, T_1 and T_2, define the qubit's stability before it collapses.

1.4 Quantum Gate Errors and Crosstalk

- Control errors arise from imprecise gate implementations.
- Crosstalk errors occur when one qubit's operations inadvertently affect another.
- Measurement errors introduce bias in final state readout.

1.5 Ion Trap Errors and Environmental Perturbations

- Shuttle operation noise: In ion-trap quantum computers, ions are physically moved between traps, introducing motion-related decoherence.
- External field disruptions: Stray electromagnetic fields and temperature fluctuations introduce unwanted energy shifts, affecting computation.

2. Adversarial Quantum Noise and Security Risks

Viewing noise as an adversarial act introduces security threats similar to fault injections in classical ML[50]. Adversaries may deliberately introduce errors to:

- Corrupt computations (e.g., manipulate quantum key distribution).
- Mislead quantum learning models by introducing structured noise.
- Introduce hardware backdoors via controlled error injection attacks.

These threats necessitate robust error mitigation techniques.

3.2.4 Noise Mitigation Strategies and Error Correction

Quantum error correction (QEC) is fundamental to overcoming hardware noise [51]. Common methods include:

1. Quantum Error Correcting Codes (QECC)
    - Shor code: Protects against bit-flip and phase-flip errors using redundant encoding: $|0\rangle \rightarrow |000\rangle, |1\rangle \rightarrow |111\rangle$
    - Surface codes: Widely used in superconducting qubits for fault-tolerant computing.
2. Quantum Error Mitigation (QEM)
    - Zero-noise extrapolation (ZNE) estimates and cancels errors post-computation.
    - Dynamical decoupling (DD) uses periodic pulses to counteract environmental noise.
3. Fault-Tolerant Quantum Computing (FTQC)
    - Requires logical qubits, built from many physical qubits, to correct errors without collapsing the quantum state.

DOI : 10.31695/IJERAT.2025.4.1

Realizing sensible quantum computing still depends on a basic challenge: quantum noise. Development of fault-tolerant quantum systems [52] depends on an awareness of error models, security issues, and error correction methods. Reducing hostile quantum noise is a developing area of study guaranteeing dependable and safe quantum processing [53].

4. RESEARCH METHODOLOGY

Following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) approach, a methodical search was undertaken to guarantee an objective and thorough literature evaluation. In academic research, the PRISMA [54] technique is a methodical strategy intended to minimize selection bias and methodically find, filter, and analyse relevant material..

4.1 PRISMA Framework and Methodology

The PRISMA framework consists of four key stages:

1. Identification:
    - ❖ A broad search of academic databases (e.g., IEEE Xplore, Springer, ACM Digital Library, PubMed, arXiv) is conducted to collect relevant studies.
    - ❖ Keywords, Boolean logic, and controlled vocabularies (e.g., MeSH terms in biomedical studies) are used.
2. Screening:
    - ❖ Duplicates are removed.
    - ❖ Titles and abstracts are screened for relevance to the research question.
3. Eligibility Assessment:
    - ❖ Full-text articles are reviewed based on predefined inclusion and exclusion criteria.
    - ❖ Bias and methodological rigor are evaluated.
4. Inclusion:
    - ❖ Final studies are selected for qualitative and quantitative analysis.

This process ensures transparency, reproducibility, and reliability in literature selection.

4.2 Literature Search Strategy and Execution

The literature review process was conducted using two search methods, executed sequentially:

1. Primary Search Method
    - A structured query was applied to peer-reviewed academic databases.
    - Search filters were applied to refine the results based on publication year, relevance, citation impact, and peer-review status.
2. Secondary Search Method
    - A snowballing approach was used, where citations and references from initial studies were examined.

DOI : 10.31695/IJERAT.2025.4.1

- This method enhances coverage and retrieval of key foundational papers.

Figure 1. illustrates the flow of literature selection, depicting PRISMA-based filtering from the initial dataset to the final included studies.

By employing a systematic and multi-stage selection process, the literature review minimizes information bias, ensuring an objective synthesis of existing research.

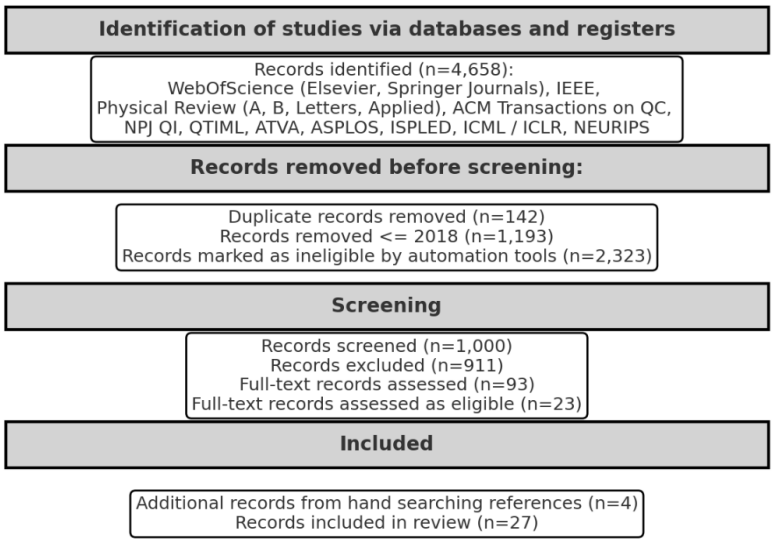

Figure 1: Documentation of search process [45]

5. QUANTUM VULNERABILITIES

Although quantum computing offers fresh computational possibilities, it also creates weaknesses and security concerns that have to be addressed [55]. Hardware constraints, noise-induced mistakes, algorithmic flaws, and adversarial assaults [56] create these issues.

5.1 Hardware-Induced Vulnerabilities

Hardware defects, which cause major calculation mistakes, essentially limit quantum computing. Characterized by short coherence periods, T1 (energy relaxation time) and T2 (dephasing time), decoherence and qubit instability is one of the most important difficulties. These values restrict the depth and precision of quantum calculations by defining how long a qubit maintains its quantum state before external interactions induce information loss [55, 57]. Quantum gate flaws are yet another main cause of mistakes. Unitary transformations are used in quantum computations, however in practical hardware control noise and manufacturing flaws cause gates to not be exactly performed. Particularly in extended quantum circuits, even tiny variations in gate quality cause cumulative mistakes that degrade computational dependability.

Another similar problem is crosstalk mistakes, in which actions on one qubit unwittingly affect another. Residual electromagnetic coupling between qubits causes this effect by adding unplanned quantum correlations. In multi-qubit entangled states, where exact control over interactions is required to preserve algorithmic correctness [58], crosstalk errors are more troublesome. Moreover, in quantum readout measurement errors provide a major obstacle. Quantum measurements project the state of a qubit into either

DOI : 10.31695/IJERAT.2025.4.1

|0⟩ or |1⟩, but noise in the measuring process may cause misread results and hence introduce biases in probabilistic quantum computing. These mistakes in detector inefficiencies, thermal noise, and poor sensor calibration finally influence quantum algorithms depending on high-precision state estimate. To increase quantum hardware stability, addressing these weaknesses calls for developments in quantum error correction (QEC), fault-tolerant quantum designs, and better qubit production methods.

5.2 Adversarial Quantum Attacks

Although it offers hitherto unheard-of processing capacity, quantum computing is vulnerable to adversarial assaults that might control quantum calculations and jeopardize quantum security. Like fault injection attacks in classical systems, one of the main attack points is quantum noise injection. Adversaries may purposefully add noise to a quantum system, hence distorting quantum states and producing false computing results [55]. In quantum variational algorithms and quantum machine learning models, where minor perturbations may produce notable misclassifications [56], this is especially troublesome.

Quantum side-channel attacks, in which attackers use inadvertent interactions between qubits and their surroundings to harvest sensitive data, provide another class of security concerns. Quantum side-channel attacks may use state collapse probabilities, leakage via crosstalk, or indirect qubit interactions to infer computational states without directly measuring them unlike conventional side-channel attacks, which usually exploit time or power consumption [58]. Targeting especially quantum cryptography systems meant to guarantee safe communication, Quantum Key Distribution (QKD) Attacks Using flaws in single-photon sources used in BB84 QKD, the Photon Number Splitting (PNS) Attack lets an eavesdropper intercept portion of the quantum key without appreciable disturbance of the quantum states. The Man-in- the- Middle Attack on Quantum Channels is another important weakness wherein an attacker modulates entangled quantum states, therefore influencing the quantum communication process and maybe changing encryption keys [59]. Future quantum networks have to include quantum cryptographic resilience methods such decoy-state protocols, quantum error correction, and quantum-resistant authentication systems in order to reduce these hazards...

5.3 Algorithmic Vulnerabilities

Although they provide computing benefits, quantum algorithms have intrinsic flaws that might be used maliciously or advantageously to compromise conventional cryptographic security [60]. In Quantum Machine Learning (QML), where adversarial assaults may alter quantum data representations and result in misclassifications and biased predictions, one main issue raises itself. Small perturbations in input data can have a major impact on the output of a model in classical machine learning; similarly, adversarial changes to quantum states can distort probability amplitudes, so changing computational outcomes in Quantum Neural Networks (QNNs) and Variational Quantum Circuits (VQCs). These perturbations may be deliberately engineered to take advantage of flaws in quantum feature mapping and encoding, therefore making QML-based classifiers unreliable in important uses [61]. Quantum Cryptanalysis, especially using Shor's Algorithm, which compromises extensively used public-key cryptography systems as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), raises more basic mathematical vulnerabilities. Using the Quantum Fourier Transform (QFT) and quantum period-finding, Shor's method factors big numbers in polyn time.:

$$N=p\times q$$

where N is a big semiprime integer. By running in sub-exponential time, the most well-known classical methods for integer factorization—General Number Field Sieve (GNFS)—run RSA encryption safe against

DOI : 10.31695/IJERAT.2025.4.1

classical assaults. But Shor's Algorithm simplifies the complexity to O(n3), making RSA encryption breakable once fault-tolerant quantum computers find application. Analogous vulnerability to quantum assaults exists in ECC, which depends on the complexity of the elliptic curve discrete logarithm problem (ECDLP). Post-quantum cryptographic techniques like lattice-based encryption, hash-based signatures, and quantum-resistant key exchange protocols are under development to offset quantum computational hazards [62].

5.4 Countermeasures and Future Security

Mitigating hardware, algorithmic, and adversarial weaknesses as quantum computing develops calls for a mix of fault-tolerant design, error correction, and cryptography breakthroughs. Quantum Error Correction (QEC) is the main approach to solve quantum mistakes as it shields quantum calculations from hardware noise, decoherence, and gate faults. Unlike conventional error correction, QEC detects and fixes faults without collapsing quantum states by use of redundant logical qubit encoding using many physical qubits. The most often investigated QEC methods are the Shor Code, which redundantly encodes quantum information [63] and the Surface Code, which may fix single-qubit mistakes by encoding a logical qubit into a lattice of several physical qubits.

Post-Quantum Cryptography (PQC), which aims at creating cryptographic systems resistant to quantum assaults, is another necessary security precaution. New encryption methods include lattice-based cryptography, code-based cryptography, and multivariate poisson cryptosystems are being developed to stay safe even against strong quantum adversaries because Shor's Algorithm compromises RSA, ECC, and other conventional cryptographic schemes. Fault-tolerant quantum computing (FTQC), which combines QEC with logical qubits to execute calculations without building mistakes, guarantees the long-term dependability of quantum computations. By use of extensive universal quantum computing, FTQC seeks to guarantee consistent operation of quantum algorithms even in the presence of noise [64]. To reduce possible security concerns and computational instabilities, achieving secure and scalable quantum computing will need for strong hardware optimizations, quantum-safe cryptography frameworks, and quantum control method developments.

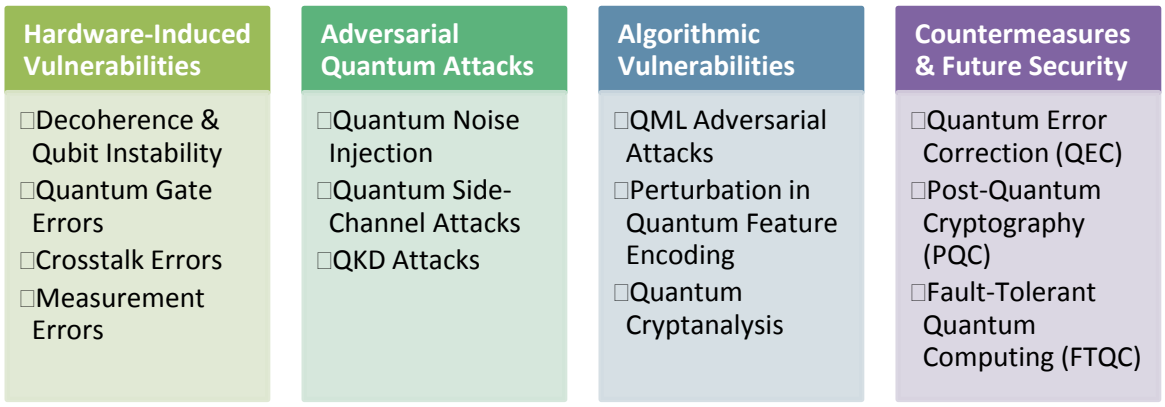

Figure 2: A Taxonomy map outlining the main QML vulnerabilities.

DOI : 10.31695/IJERAT.2025.4.1

6. QUANTUM DEFENCES

Adversarial attacks may violate model integrity, distort quantum computations, and leak important quantum states [65]. Quantum Machine Learning (QML) models are so vulnerable. Strong quantum encoding, adversarial training, quantum error correction, and cryptographic protections taken together define effective defenses against such assaults.

6.1 Robust Quantum Data Encoding

Strong quantum feature encoding methods that maintain data integrity and reduce vulnerability to adversary alterations define resilience to adversarial perturbations in Quantum Machine Learning (QML). Underlying QML models, quantum feature encoding maps classical data into quantum states in a Hilbert space. By adding redundancy, encoding techniques as Amplitude Embedding and Angle Encoding may be altered to make QML models less vulnerable to perturbations in quantum state preparation [66]. These changes guarantee that small changes in input data have no appreciable effect on the final quantum state, hence strengthening resilience.

Defensive encoding—error-detecting embeddings that translate classical data into a higher-dimensional Hilbert space—is one efficient security method. Adversarial perturbations lose their efficacy by raising the dimensionality of the feature space as they must induce many more distortions to control the encoded quantum state. This method guarantees structural integrity of the quantum representation even under hostile intervention. Quantum feature smoothing—which uses quantum noise-resistant operations to quantum states—is another way to increase resilience. These changes provide a buffer against minor perturbations, hence lowering the susceptibility of quantum models to adversarial noise. This idea is similar to adversarial training in conventional neural networks, wherein models are taught with noisy or disturbed inputs to boost their resistance [67]. Combining these methods helps QML models to grow naturally more resistant to adversarial assaults, hence guaranteeing improved stability and security in quantum computing.

6.2 Adversarial Training in QML

Extensive use of adversarial training, a well-known defensive mechanism in classical machine learning, to Quantum Machine Learning (QML) strengthens model resilience against quantum adversarial assaults. This method trains quantum models on both clean and adversarially disturbed quantum states, therefore allowing them to generalize better and withstand hostile perturbations. This approach is especially successful in Parameterized Quantum Circuits (PQCs), in which adversary inputs may control the quantum state development, hence producing erroneous computations or wrong classifications [68]. Variational circuit robustness—training PQCs on a hybrid dataset including both clean and adversarially disturbed quantum states—is a fundamental component of adversarial training in QML. The quantum circuit learns to discriminate between natural and adversarially changed quantum data by exposing the model to these modified states during training, hence reducing its sensitivity to minor perturbations. This method guarantees that adversarial changes have no appreciable effect on computing results, hence enhancing the stability of quantum variational methods.

Adaptive Noise Injection is another useful protection strategy wherein tiny randomized quantum disturbances are purposefully injected during training. This approach forces the model to develop robust quantum representations that are less sensitive to small adversarial fluctuations, hence preventing overfitting to adversarial cases. By efficiently smoothing the loss landscape of QML models, adaptive noise injection lowers their susceptibility to adversarial optimization strategies that take use of abrupt decision boundaries

DOI : 10.31695/IJERAT.2025.4.1

in quantum feature space [69]. These methods taken together support the security and resilience of QML models in hostile settings.

6.3 Quantum Error Correction (QEC) for Model Integrity

Often using hardware noise and qubit instability, quantum adversarial assaults cause incorrect calculations in Quantum Machine Learning (QML) models. Protection of quantum computations against these adversarially generated quantum disturbances depends critically on quantum error correction (QEC), hence guaranteeing the dependability and stability of quantum circuits. Any hostile interference, including bit-flip errors, phase-flip errors, or decoherence effects, may greatly reduce model performance as QML models depend on coherent quantum states for processing. Maintaining quantum model integrity [70] depends on using error correcting techniques.

Surface codes and stabilizer codes—which guard quantum states against bit-flip and phase-flip errors—are among the most powerful QEC methods available. Surface codes distribute quantum information repeatedly to discover and fix faults by encoding logical qubits into a vast network of physical qubits. These algorithms help QML models to be robust to minor adversarial perturbations, hence preventing attackers from adding modest quantum noise to control computational results [71]. Apart from error-correcting codes, fault-tolerant variational quantum circuits (VQCs) improve the resilience of QML by use of logical qubits resistant to adversarial noise. Error-corrected quantum gates used in these fault-tolerant circuits help to decrease the spread of adversarial perturbations across the computation. Designing QML models with built-in QEC methods helps to greatly reduce adversarial changes to quantum computations, hence guaranteeing consistent and safe execution of quantum learning algorithms even in the face of deliberate or ambient noise [72].

6.4 Cryptographic Defences and Quantum Secure Learning

In Quantum Machine Learning (QML), security calls for cryptographic protections guarding against model manipulation, adversarial quantum computations, and data leaks. Unlike classical models, QML systems depend on quantum superposition, entanglement, and probabilistic measurement, so they are susceptible to assaults via quantum information leakage or computational process manipulation. Secure learning systems have to be included into QML systems if we are to mitigate these hazards thus guaranteeing data confidentiality, model integrity, and resistance to hostile intervention [73]. Quantum homomorphic encryption (QHE), which enables quantum computations on encrypted quantum states without disclosing the underlying data, is among the most exciting cryptographic techniques available. This lets QML models handle encrypted inputs, therefore preventing attackers from deducing model parameters, quantum states, or training data. Unlike conventional homomorphic encryption, which suffers from computational inefficiencies, QHE runs within a quantum computational framework using quantum mechanics to provide effective secure computing [74]. Sensitive quantum data stays completely safeguarded by implementing QHE even on possibly untrustworthy quantum hardware.

The use of Quantum Authentication Protocols is yet another essential security feature. These protocols ensure that the predictions and computations made by QML models are accurate and trustworthy. Verification of the outcomes of quantum inference may be accomplished via the use of techniques such as quantum digital signatures. This ensures that attackers are unable to manipulate the outputs of the model or introduce alterations that are not approved [75]. Quantum machine learning (QML) models are able to develop resistance against model hijacking, illegal quantum access, and hostile data manipulations via the incorporation of cryptographic verification methods. This helps to ensure that quantum-based learning systems are both legitimate and private.

DOI : 10.31695/IJERAT.2025.4.1

6.5 Quantum Adversarial Detection and Countermeasures

Maintaining the integrity of Quantum Machine Learning (QML) models depends critically on the identification and neutralization of adversarial perturbations in Quantum Neural Networks (QNNs) and Variational Quantum Circuits (VQCs). Quantum adversarial attacks may change quantum states, change circuit parameters, or use quantum noise to decrease model performance unlike conventional adversarial attacks, which change input data. Sophisticated quantum adversarial detection and mitigating methods must be used to protect QML models against such attacks [76]. Quantum Fisher Information Analysis is one efficient method because it quantifies sensitivity in quantum parameter environments to identify hostile changes. A useful instrument for determining perturbed quantum states, the Quantum Fisher Information Matrix (QFIM) describes how little variations in quantum states influence measuring probabilities. The QFIM response differs greatly when an adversarial assault generates non-physical disturbances, therefore indicating the existence of hostile interference [77]. Through ongoing observation of these fluctuations, QML models can dynamically identify and adjust to adversarial perturbations.

Entanglement-Based Anomaly Detection is another sophisticated technique based on entanglement entropy that finds hostile interference in multi-qubit quantum systems. Quantum entanglement reflects the natural structure of quantum computing and follows predictable trends in well-structured QML models. Malicious changes introduced by an opponent cause the entanglement entropy to differ from predicted values, suggesting non-physical disturbances [78]. Monitoring entanglement features helps QML models to independently detect, flag, and reduce adversarial impact, hence guaranteeing strong and safe quantum learning.

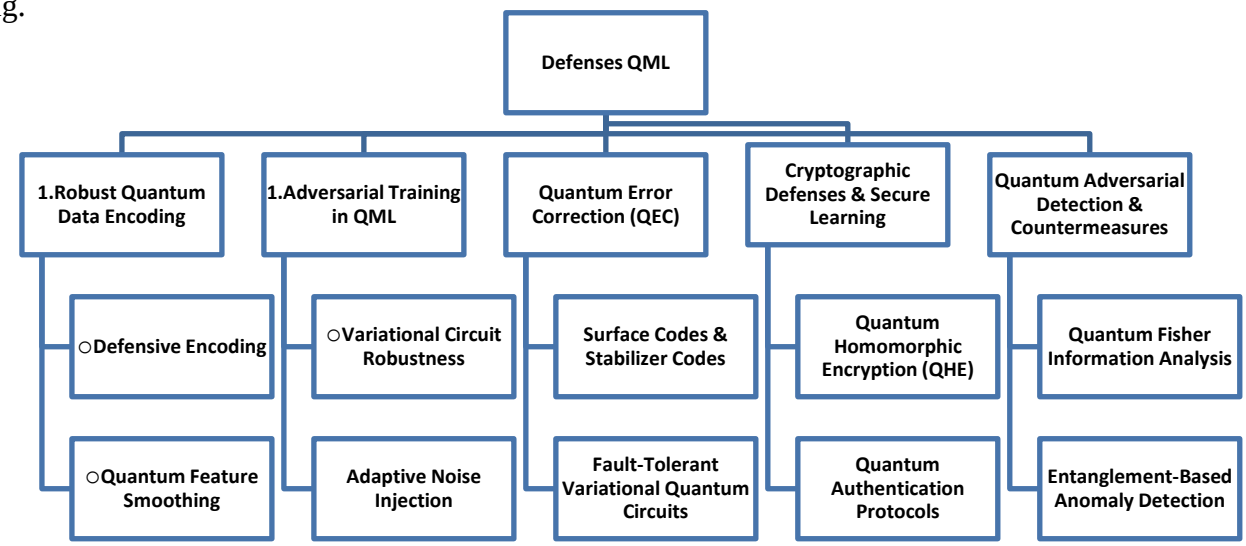

Figure 3: Diagram for Taxonomy of Defences Against Adversarial Attacks in Quantum Machine Learning (QML)

6.6 Discussion & Future Directions in QML Security

The study of vulnerabilities and defences in Quantum Machine Learning (QML) is a vital and developing field of research needing creative solutions to improve model security and robustness. The possible attack routes follow in line with the increasing sophistication of QML models, therefore a thorough knowledge of both quantum system design and its sensitivity to adversarial manipulation [79] is essential. The development of novel attack routes—especially via fault injections and intentional manipulation of quantum noise—particularly raises urgent issues. These adversarial techniques reduce computing accuracy by leveraging noise-induced decoherence, qubit instability, and cross-talk effects, hence exploiting the intrinsic

DOI : 10.31695/IJERAT.2025.4.1

fragility of quantum systems. The difficulty grows when quantum systems expand as the growth of Hilbert spaces raises the sensitivity of the model to disturbances [80]. Achieving quantum advantage while guaranteeing security and stability emphasizes the critical requirement of strong verification techniques that can effectively adapt to the complexity of big-scale quantum computing by means of a careful balancing.

Defence-wise, improving QML security calls for major developments in formal verification methods, differential privacy, and adversarial training. Although conventional adversarial training has been modified for quantum models, the special probabilistic character of quantum states calls for further improvement to address quantum-specific hazards. A fundamental idea in classical machine learning, differential privacy is still in its early phases of adaption to quantum contexts and needs careful investigation to create efficient quantum-safe implementations [81]. Furthermore offering interesting routes for mathematically exact defenses against quantum adversarial assaults are mathematical integer linear programming (MILP) verification and Lipschitz continuity analysis. Still under development in the quantum world, these techniques need further work before they become generally useful and efficient in protecting QML models [82]. Cross-disciplinary research has a bright future because hybrid defensive mechanisms combining classical and quantum security measures may provide a multi-layered security framework against adversarial attacks. Combining strong optimization systems, quantum-specific countermeasures, and conventional cryptography methods could provide creative ideas with more robustness. But first empirical research and benchmarking systems have to be developed if we are to fairly assess these strategies. Assessing the efficacy of suggested security solutions under real-world situations [83] depends on standardized datasets, attack scenarios, and assessment criteria unique to QML vulnerabilities and countermeasures.

All things considered, the direction of QML security research calls for a multidisciplinary approach combining ideas from machine learning (ML) and quantum computing (QC) to create models not only computationally strong but also safe against adversarial assaults. The research community can propel major progress toward guaranteeing the security, resilience, and practical deployment of QML systems by tackling these fundamental challenges—ranging from novel attack routes to the refining of defensive techniques and the introduction of empirical benchmarks.

7. CONCLUSION

Before they may be reasonably used in useful applications, quantum machine learning (QML) models present special security issues that have to be resolved. Quantum systems' basic characteristics—entanglement, superposition, probabilistic measurement—make them essentially distinct from conventional models and provide fresh attack surfaces that enemies may use. A hostile actor may subtly and difficultly attack the architectural integrity of a QML model, modify the intrinsic quantum noise, or use hardware-induced vulnerabilities. Although numerous defensive mechanisms have been suggested in the literature, their practical relevance and dependability require further empirical confirmation, especially in the framework of big-scale quantum systems.

Notwithstanding these security issues, QML models show natural resistance against several traditional attack paths. Several elements contribute to this resilience. First of all, the effective adaption of classical and quantum adversarial training approaches has reinforced QML models against perturbations in quantum feature space. Second, some quantum architectures—such as quanvolutional networks and quantum-enhanced Restricted Boltzmann Machines (RBMs)—have been found to show structural robustness against adversarial modifications, so reducing their sensitivity to attacks relative to conventional deep learning models. Furthermore investigated as a technique of improving differential privacy is the use of device-induced noise, thereby using the natural stochastic character of quantum measurements to hide sensitive data

DOI : 10.31695/IJERAT.2025.4.1

from adversary inference. Ultimately, QML reduces prevalent hazard in traditional deep learning, gradient inversion attacks, by means of designs that naturally safeguard sensitive data and hence stop attackers from recreating input information from gradient-based optimization processes.

The merger of Quantum Computing (QC) and Machine Learning (ML) technologies will ultimately determine the direction of QML security research as it promotes a multidisciplinary approach investigating hybrid defensive tactics. This calls for thorough empirical research, the creation of fresh benchmarking systems, and the creation of standardized datasets and assessment criteria especially fit to QML security concerns. By tackling these difficulties, scientists might endeavor to create QML models that are not only computationally efficient and strong but also safe and robust against a broad spectrum of adversarial threats.

REFERENCES

[1.] Peter W Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th annual symposium on foundations of computer science*. Ieee. 1994, pp. 124–134.

[2.] Xu, Yongchun, et al. "Quantum computing enhanced distance-minimizing data-driven computational mechanics." *Computer Methods in Applied Mechanics and Engineering* 419 (2024): 116675..

[3.] John Preskill. "Quantum computing in the NISQ era and beyond". In: *Quantum* 2 (2018), p. 79.

[4.] Wang, Youle, and Yu Luo. "Resource-efficient quantum principal component analysis." *Quantum Science and Technology* 9.3 (2024): 035031..

[5.] Aggarwal, Ada, et al. "A Detailed Overview of Quantum Computing Machine Learning Techniques." *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)*. IEEE, 2024..

[6.] Ullah, Ubaid, and Begonya Garcia-Zapirain. "Quantum machine learning revolution in healthcare: a systematic review of emerging perspectives and applications." *IEEE Access* 12 (2024): 11423-11450..

[7.] Hdaib, Moe, Sutharshan Rajasegarar, and Lei Pan. "Quantum deep learning-based anomaly detection for enhanced network security." *Quantum Machine Intelligence* 6.1 (2024): 26.

[8.] Xu, Hairun, et al. "Quantum Reinforcement Learning for real-time optimization in Electric Vehicle charging systems." *Applied Energy* 383 (2025): 125279..

[9.] Alluhaibi, Reyadh. "Quantum Machine Learning for Advanced Threat Detection in Cybersecurity." *International Journal of Safety & Security Engineering* 14.3 (2024).

[10.] Hanzo, Lajos, et al. "Quantum Information Processing, Sensing, and Communications: Their Myths, Realities, and Futures." *Proceedings of the IEEE* (2025)..

[11.] Eldar, Lior, and Sean Hallgren. "An efficient quantum algorithm for lattice problems achieving subexponential approximation factor." *arXiv preprint arXiv:2201.13450* (2022).

[12.] AbuGhanem, Muhammad, and Hichem Eleuch. "NISQ computers: a path to quantum supremacy." *IEEE Access* (2024)..

[13.] Pierre-Luc Dallaire-Demers and Nathan Killoran. "Quantum generative adversarial networks". In: *Physical Review A* 98.1 (2018), p. 012324.

[14.] Sirui Lu, Lu-Ming Duan, and Dong-Ling Deng. "Quantum adversarial machine learning". In: *Physical Review Research* 2.3 (2020), p. 033212.

[15.] Li, Guangxi. *Machine Learning Applications of Parameterized Quantum Circuits*. Diss. 2023.

[16.] Jerbi, Sofiene, et al. "Quantum machine learning beyond kernel methods." *Nature Communications* 14.1 (2023): 517.

[17.] Smaldone, Anthony M., Gregory W. Kyro, and Victor S. Batista. "Quantum convolutional neural networks for multi-channel supervised learning." *Quantum Machine Intelligence* 5.2 (2023): 41..

DOI : 10.31695/IJERAT.2025.4.1

[18.] Anil, Gautham, Vishnu Vinod, and Apurva Narayan. "Generating universal adversarial perturbations for quantum classifiers." *Proceedings of the AAAI Conference on Artificial Intelligence*. Vol. 38. No. 10. 2024..

[19.] Haoran Liao et al. "Robust in practice: Adversarial attacks on quantum machine learning". In: *Physical Review A* 103.4 (2021), p. 042427.

[20.] Zhang, Chuanyu, et al. "Quantum continual learning on a programmable superconducting processor." *arXiv preprint arXiv:2409.09729* (2024).

[21.] Amira Abbas et al. "The power of quantum neural networks". In: *Nature Computational Science* 1.6 (2021), pp. 403–409. DOI: 10.1038/s43588-021-00084-1.

[22.] Korn Sooksatra, Pablo Rivas, and Javier Orduz. "Evaluating accuracy and adversarial robustness of quanvolutional neural networks". In: *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE. 2021, pp. 152–157.

[23.] Andrea Skolik et al. "Robustness of quantum reinforcement learning under hardware errors". In: *EPJ Quantum Technology* 10.1 (2023), pp. 1–43.

[24.] Huijgen, Onno, et al. "Training quantum Boltzmann machines with the β-variational quantum eigensolver." *Machine Learning: Science and Technology* 5.2 (2024): 025017.

[25.] West, Maxwell T., et al. "Towards quantum enhanced adversarial robustness in machine learning." *Nature Machine Intelligence* 5.6 (2023): 581-589..

[26.] Hsin-Yuan Huang et al. "Power of data in quantum machine learning". In: *Nature Communications* 12.1 (2021). DOI: 10.1038/s41467-021-22539-9. URL: https: //doi.org/10.1038%2Fs41467-021-22539-9.

[27.] Thakur, Vikram Singh, et al. "Quantum Error Correction Codes in Consumer Technology: Modelling and Analysis." *IEEE Transactions on Consumer Electronics* (2024)..

[28.] Nadkarni, Priya J., Narayanan Rengaswamy, and Bane Vasić. "Tutorial on quantum error correction for 2024 quantum information knowledge (quik) workshop." *arXiv preprint arXiv:2407.12737* (2024)..

[29.] Strasberg, Philipp, Teresa E. Reinhard, and Joseph Schindler. "First principles numerical demonstration of emergent decoherent histories." *Physical Review X* 14.4 (2024): 041027..

[30.] Hashim, Akel, et al. "Benchmarking quantum logic operations relative to thresholds for fault tolerance." *npj Quantum Information* 9.1 (2023): 109..

[31.] Das, Subrata, Avimita Chatterjee, and Swaroop Ghosh. "Investigating impact of bit-flip errors in control electronics on quantum computation." *2025 38th International Conference on VLSI Design and 2024 23rd International Conference on Embedded Systems (VLSID)*. IEEE, 2025..

[32.] Menta, Roberto, et al. "Globally driven superconducting quantum computing architecture." *Physical Review Research* 7.1 (2025): L012065..

[33.] Schoenberger, Daniel, et al. "Shuttling for scalable trapped-ion quantum computers." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (2024)..

[34.] Ezratty, Olivier. "Perspective on superconducting qubit quantum computing." *The European Physical Journal A* 59.5 (2023): 94..

[35.] Alluhaibi, Reyadh. "Quantum Machine Learning for Advanced Threat Detection in Cybersecurity." *International Journal of Safety & Security Engineering* 14.3 (2024)..

[36.] Rath, Minati, and Hema Date. "Quantum data encoding: A comparative analysis of classical-to-quantum mapping techniques and their impact on machine learning accuracy." *EPJ Quantum Technology* 11.1 (2024): 72.

[37.] Schalkers, Merel A., and Matthias Möller. "On the importance of data encoding in quantum Boltzmann methods." *Quantum Information Processing* 23.1 (2024): 20.

DOI : 10.31695/IJERAT.2025.4.1

[38.] Sierra-Sosa, Daniel, Soham Pal, and Michael Telahun. "Data rotation and its influence on quantum encoding." *Quantum Information Processing* 22.1 (2023): 89.

[39.] Majji, Sathwik Reddy, Avinash Chalumuri, and B. S. Manoj. "Quantum approach to image data encoding and compression." *IEEE Sensors Letters* 7.2 (2023): 1-4.

[40.] Weigold, Manuela, et al. "Expanding data encoding patterns for quantum algorithms." *2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C)*. IEEE, 2021.

[41.] Bravo-Prieto, Carlos. "Quantum autoencoders with enhanced data encoding." *Machine Learning: Science and Technology* 2.3 (2021): 035028.

[42.] Shin, Seongwook, Yong-Siah Teo, and Hyunseok Jeong. "Exponential data encoding for quantum supervised learning." *Physical Review A* 107.1 (2023): 012422.

[43.] Hur, Tak, Leeseok Kim, and Daniel K. Park. "Quantum convolutional neural network for classical data classification." *Quantum Machine Intelligence* 4.1 (2022): 3.

[44.] Sharma, Siddhartha, and N. Renugadevi. "Survey of encoding techniques for quantum machine learning." *Cybernetics and Physics* 13.2 (2024).

[45.] Huang, Hsin-Yuan, et al. "Power of data in quantum machine learning." *Nature communications* 12.1 (2021): 2631.

[46.] Darras, Tom, et al. "A quantum-bit encoding converter." *Nature Photonics* 17.2 (2023): 165-170.

[47.] Cerezo, Marco, et al. "Challenges and opportunities in quantum machine learning." *Nature computational science* 2.9 (2022): 567-576.

[48.] West, Maxwell T., et al. "Towards quantum enhanced adversarial robustness in machine learning." *Nature Machine Intelligence* 5.6 (2023): 581-589.

[49.] Stein, Samuel A., et al. "A hybrid system for learning classical data in quantum states." *2021 IEEE International Performance, Computing, and Communications Conference (IPCCC)*. IEEE, 2021.

[50.] Chen, Samuel Yen-Chi, et al. "Quantum convolutional neural networks for high energy physics data analysis." *Physical Review Research* 4.1 (2022): 013231.

[51.] Schuld, Maria. "Supervised quantum machine learning models are kernel methods." *arXiv preprint arXiv:2101.11020* (2021).

[52.] Haug, Tobias, Chris N. Self, and Myungshik S. Kim. "Quantum machine learning of large datasets using randomized measurements." *Machine Learning: Science and Technology* 4.1 (2023): 015005.

[53.] Bokhan, Denis, et al. "Multiclass classification using quantum convolutional neural networks with hybrid quantum-classical learning." *Frontiers in Physics* 10 (2022): 1069985.

[54.] LA Kahale et al. “Extension of the PRISMA 2020 statement for living systematic reviews (LSRs): protocol [version 2; peer review: 1 approved]”. In: *F1000Research* 11.109 (2022). DOI: 10 . 12688 / f1000research.75449.2.

[55.] Cheng Chu et al. “QTROJAN: A Circuit Backdoor Against Quantum Neural Networks”. In: *ICASSP 20232023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE. 2023, pp. 1–5.

[56.] Cheng Chu et al. “QDoor: Exploiting Approximate Synthesis for Backdoor Attacks in Quantum Neural Networks”. In: *2023 IEEE International Conference on Quantum Computing and Engineering (QCE)*. Vol. 1. IEEE. 2023, pp. 1098–1106.

[57.] Abdullah Ash Saki, Mahabubul Alam, and Swaroop Ghosh. “Impact of noise on the resilience and the security of quantum computing”. In: *2021 22nd International Symposium on Quality Electronic Design (ISQED)*. IEEE. 2021, pp. 186–191.

DOI : 10.31695/IJERAT.2025.4.1

[58.] Mehmood, Abid, et al. "Advances and vulnerabilities in modern cryptographic techniques: A comprehensive survey on cybersecurity in the domain of machine/deep learning and quantum techniques." *IEEE access* 12 (2024): 27530-27555.

[59.] Mehdi Sadi et al. “Special Session: On the Reliability of Conventional and Quantum Neural Network Hardware”. In: *2022 IEEE 40th VLSI Test Symposium (VTS)*. 2022, pp. 1–12. DOI: 10.1109/VTS52500.2021.9794194.

[60.] Upadhyay, Suryansh, and Swaroop Ghosh. "Quantum Quandaries: Unraveling Encoding Vulnerabilities in Quantum Neural Networks." *arXiv preprint arXiv:2502.01486* (2025)..

[61.] Sadiq, Samina, and Aynur Unalp. "Quantum-Safe Cyber Security: Preparing SOC Operations for Post-Quantum Threats." (2025)..

[62.] Gitonga, Charles Kinyua. "The Impact of Quantum Computing on Cryptographic Systems: Urgency of Quantum-Resistant Algorithms and Practical Applications in Cryptography." *European Journal of Information Technologies and Computer Science* 5.1 (2025): 1-10.

[63.] Jowarder, Rafiul Azim, and Sawgat Jahan. "Quantum computing in cyber security: Emerging threats, mitigation strategies, and future implications for data protection." *World Journal of Advanced Engineering Technology and Sciences* 13.1 (2024): 330-339. .

[64.] Singla, Arun. "Cloud Security in the Age of Quantum Computing: Risks and Countermeasures." *Shodh Sagar Journal of Artificial Intelligence and Machine Learning* 1.3 (2024): 10-13..

[65.] Khan, Sadik, et al. "Quantum Computing And Its Implications For Cybersecurity: A Comprehensive Review Of Emerging Threats And Defenses." *Nanotechnology Perceptions* 20 (2024): S13..

[66.] Chu, Cheng, et al. "Iqgan: Robust quantum generative adversarial network for image synthesis on nisq devices." *ICASSP 2023-2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2023..

[67.] Li, Guangxi, et al. "Concentration of data encoding in parameterized quantum circuits." *Advances in Neural Information Processing Systems* 35 (2022): 19456-19469..

[68.] Kundu, Satwik, and Swaroop Ghosh. "Adversarial poisoning attack on quantum machine learning models." *arXiv preprint arXiv:2411.14412* (2024)..

[69.] Li, Bacui, et al. "Computable Model-Independent Bounds for Adversarial Quantum Machine Learning." *arXiv preprint arXiv:2411.06863* (2024). .

[70.] Thakur, Vikram Singh, et al. "Quantum Error Correction Codes in Consumer Technology: Modelling and Analysis." *IEEE Transactions on Consumer Electronics* (2024)..

[71.] Chatterjee, Avimita, Koustubh Phalak, and Swaroop Ghosh. "Quantum error correction for dummies." *2023 IEEE International Conference on Quantum Computing and Engineering (QCE)*. Vol. 1. IEEE, 2023..

[72.] Christoph Hirche, Cambyse Rouzé, and Daniel Stilck França. “Quantum differential privacy: An information theory perspective”. In: *IEEE Transactions on Information Theory* (2023).

[73.] Aditya Sahdev and Mehul Kumar. *Adversarial Robustness based on Randomized Smoothing in Quantum Machine Learning*. 2023.

[74.] Mehmood, Abid, et al. "Advances and vulnerabilities in modern cryptographic techniques: A comprehensive survey on cybersecurity in the domain of machine/deep learning and quantum techniques." *IEEE access* 12 (2024): 27530-27555. .

[75.] Nicola Franco et al. “Quantum Robustness Verification: A Hybrid Quantum-Classical Neural Network Certification Algorithm”. In: *2022 IEEE International Conference on Quantum Computing and Engineering (QCE)*. IEEE. 2022, pp. 142–153.

DOI : 10.31695/IJERAT.2025.4.1

[76.] Lu, Sirui, Lu-Ming Duan, and Dong-Ling Deng. "Quantum adversarial machine learning." *Physical Review Research* 2.3 (2020): 033212..

[77.] Shen, Lijiong, and Christian Kurtsiefer. "Countering detector manipulation attacks in quantum communication through detector self-testing." *APL Photonics* 10.1 (2025). .

[78.] Upadhyay, Suryansh, and Swaroop Ghosh. "Stealthy swaps: Adversarial swap injection in multi-tenant quantum computing." *2024 37th International Conference on VLSI Design and 2024 23rd International Conference on Embedded Systems (VLSID)*. IEEE, 2024..

[79.] Ji Guan, Wang Fang, and Mingsheng Ying. "Robustness verification of quantum classifiers". In: *Computer Aided Verification: 33rd International Conference, CAV 2021, Virtual Event, July 20–23, 2021, Proceedings, Part I 33*. Springer. 2021, pp. 151–174.

[80.] Rishiwal, Vinay, et al. "A New Alliance of Machine Learning and Quantum Computing: Concepts, Attacks, and Challenges in IoT Networks." *IEEE Internet of Things Journal* (2025)..

[81.] Singh, Harbaksh. "9 Future Directions and Challenges, Quantum Supremacy, and Beyond." *Quantum Technology Applications, Impact, and Future Challenges* (2025): 141.

[82.] Sonavane, Arnav, et al. "Quantum machine learning models in healthcare: future trends and challenges in healthcare." *Quantum Computing for Healthcare Data* (2025): 167-187..

[83.] Bhattacharya, Pronaya, and Ashwin Verma. "Quantum-assisted graph networks: Algorithmic innovations and optimization strategies for large scale social communities." *Applied Graph Data Science*. Morgan Kaufmann, 2025. 151-165.

DOI : 10.31695/IJERAT.2025.4.1