Software: Practice and Experience

WILEY

SPECIAL ISSUE Quantum Computing and Its Application on Artificial Intelligence and Intelligent Software

SPECIAL ISSUE PAPER OPEN ACCESS

Quantum Machine Learning for Cybersecurity: A Taxonomy and Future Directions

Siva Sai[1] | Ishika Goyal[2] | Shubham Sharma[3] | Sri Harshita Manuri[4] | Vinay Chamola[3] | Rajkumar Buyya[5]

[1]Department of Electrical and Computer Engineering, National University of Singapore, Singapore, Singapore | [2]Department of Computer Science and Engineering, Birla Institute of Technology and Science, Pilani, Pilani Campus, Pilani, Rajasthan, India | [3]Department of Electrical and Electronics Engineering, Birla Institute of Technology and Science, Pilani, Pilani Campus, Pilani, Rajasthan, India | [4]Department of Computer Science and Engineering, Birla Institute of Technology and Science, Pilani, Hyderabad Campus, Hyderabad, India | [5]Quantum Cloud Computing and Distributed Systems (qCLOUDS) Laboratory, School of Computing and Information Systems, The University of Melbourne, Melbourne, Australia

Correspondence: Siva Sai (siva.sai@nus.edu.sg)

Received: 17 December 2025 | **Revised:** 23 July 2026 | **Accepted:** 17 August 2026

ABSTRACT

Context: The rapid increase in cyber threats, coupled with increasingly sophisticated attack strategies and the exponential growth of data in recent years, has exposed significant limitations in classical machine learning, rule-based, and signature-based defense mechanisms. These approaches are often unable to scale or adapt effectively to evolving threat landscapes.

Objective: As a result, Quantum Machine Learning (QML) has emerged as a promising alternative, leveraging computational principles from quantum mechanics. QML enables more expressive encoding and efficient processing of high-dimensional data, offering potential advantages for complex cybersecurity tasks.

Method: This survey provides a comprehensive overview of QML techniques relevant to the domain of security, such as Quantum Neural Networks (QNNs), Quantum Support Vector Machines (QSVMs), Variational Quantum Circuits (VQCs), and Quantum Generative Adversarial Networks (QGANs), and discusses the contributions of this paper in relation to existing research in the field and how it improves over them.

Results: It also maps these methods across supervised, unsupervised, and generative learning paradigms, as well as to core cybersecurity tasks, including intrusion and anomaly detection, malware and botnet classification, and encrypted-traffic analytics. It also discusses their application in cloud computing security, where QML can enhance secure, scalable operations.

Conclusion: Many limitations of QML in the domain of cybersecurity have also been discussed, along with the directions for addressing them.

1 | Introduction

Digital infrastructure has expanded rapidly in the last decade. While this has led to better connectivity and delivery of service, it has also resulted in increased exposure to complex cyber threats. In modern economies, various systems such as critical infrastructure, global financial rails, healthcare platforms, cloud services, and billions of consumer and industrial IoT devices are all tightly interdependent [1]. These interdependencies make them more prone to the propagation of failures and adversaries. Large-scale data breaches and targeted operations are common in recent attack operations, including state-sponsored advanced persistent threats (APTs), with increasing persistence, operational security, and automation. Furthermore, the availability of offensive tools and artificial intelligence has shortened development cycles of attackers. Novel intrusion techniques take less time and effort

to develop. Rule, signature, and classical machine learning based approaches cannot keep up with the adapting adversaries. These adversaries can manipulate features, blend with background traffic and shift their tactics across kill-chain stages. The defensive capacities are severely outmatched in front of the agility of the attackers. Thus, architectures that deliver low-latency detection, strong generalization to previously unseen behavior, and scalable operation under realistic compute and energy budgets are needed [2–4].

QML combines statistical learning with quantum computation. It performs especially well for high-dimensional pattern recognition and decision-making tasks [5]. Some QML pipelines use a combination of quantum and classical methods for preprocessing and postprocessing steps. QML encodes data using parameterized quantum circuits, leveraging superposition and entanglement that result in rich feature maps and fast kernel evaluations, which are hard to emulate classically. In the domain of cybersecurity, where signals are noisy, non-stationary, and maliciously distorted, QML representations can improve discrimination between benign variability and subtle malicious behavior. The limitations of traditional signature and rule-based defenses are the reason for this interest in QML-based techniques [6]. Thus, we present a systematic evaluation of QML techniques against strong classical baselines in this work.

QML has promising potential in addressing high-dimensional inference and optimization with fewer effective computational steps than strong classical baselines [7]. Conventional pipelines in cybersecurity telemetry struggle to keep pace with the volume, speed, and diversity of data generated from network flows, system logs, endpoint events, and threat intelligence feeds. A hybrid approach of quantum and classical techniques can leverage rich feature maps and kernel evaluations. This can reveal weak cross-modal correlations and rare-event structures in near real-time. Adversaries use techniques such as code obfuscation, multi-stage social engineering, and AI-enabled automation. The detectors for these adversaries should generalise under distribution shift and adversarial manipulation. Previous studies have indicated that quantum-based classifiers, which utilise flow-level statistics without payload decryption, can effectively detect anomalies in encrypted traffic [8]. Thus, they are able to preserve privacy without the detection utility having to suffer. Generative models based on quantum computing can simulate realistic attack traces and counterfactual scenarios, making them excellent for red-team training and pre-deployment stress testing. QML approaches are not only good at detection but also at combinatorial and stochastic optimization, such as key-rotation scheduling and attack-graph path forecasting. They also shine in the timely allocation of defense resources across cloud edge and large-scale IoT tiers, especially when there is a limited budget, and allocation needs to be done in a resource-aware manner [9, 10]. The taxonomy of QML algorithms for the domain of cybersecurity have been summarized in Figure 1.

The combined capabilities highlighted above show how QML plays a key role in future advancements in cybersecurity. This review aims to critically evaluate the real-world impacts of QML in closing gaps in cyber-threat detection, incident response, and system resilience, covering supervised, unsupervised, as well as hybrid quantum–classical modes. It summarises findings from previous real-world and experimental QML deployments. It also identifies and explains the typical system architectures and quantum data-encoding methods. This review also discusses practical limitations that arise from things such as noise and scaling issues in current quantum hardware, the overhead caused by feature-mapping processes, and optimization difficulties specific to quantum models. It also discusses the evaluation framework and assessment practices specifically tailored for cybersecurity, such as leakage-aware dataset splits, resource-accounted metrics, and robustness analyzes against adaptive adversaries that result in credible comparisons with strong classical baselines. The objective of this review is to determine the conditions in which QML can deliver substantial gains over baseline methods and to propose a research and deployment roadmap for scalable, privacy-aware, and practically deployable security solutions.

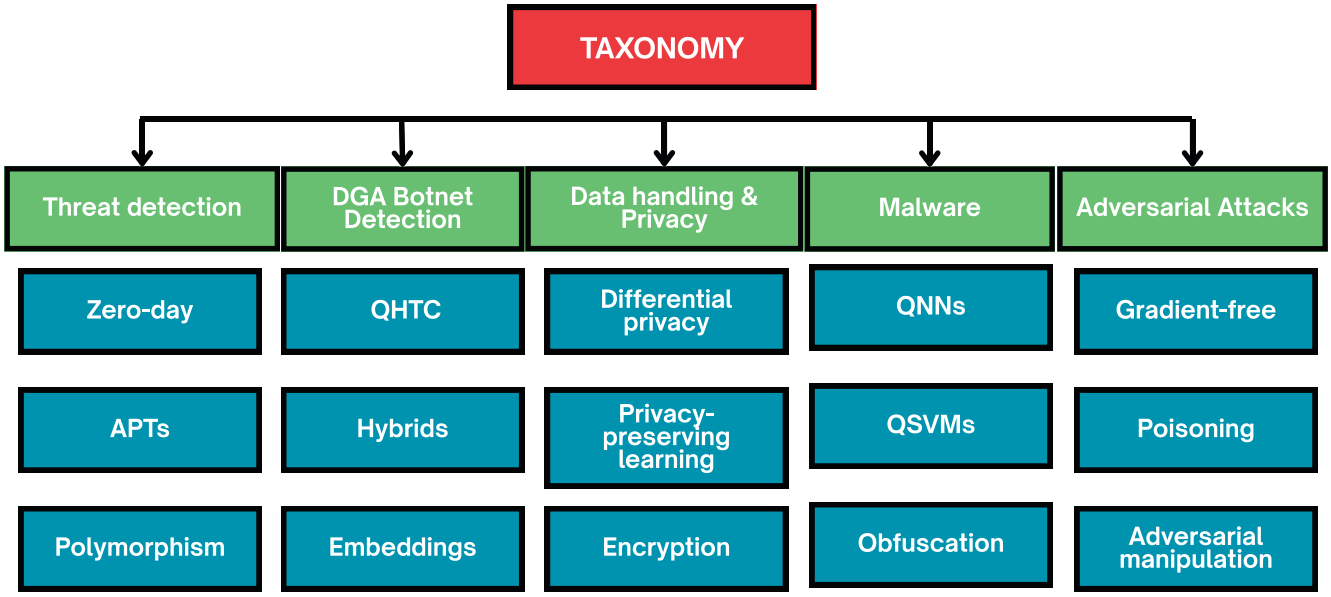

FIGURE 1 | Taxonomy of QML algorithms for cybersecurity.

2 | Related Work

QML has recently emerged as a novel and transformative technology, addressing numerous challenging problems associated with cybersecurity [1, 11]. Integrating the computational advantages of quantum computing with the adaptive learning capabilities of artificial intelligence. QML spans across various domains. Recently, numerous studies have explored this technology, offering varying depths of insight.

In 2024, Nguyen et al. [12] presented a systematic review of 32 studies in QML. In their review, they did a thorough analysis of novel algorithms like QNNs and QSVMs for various applications. Their study, although methodologically strong, focused on the principles of the technology and did not specifically extend into the field of cybersecurity. Ganapathy [13] focused their work in the domain of cybersecurity. They analyze algorithms such as QSVM, QNN, and quantum principal component analysis (QPCA), specifically for anomaly detection. They also analyzed the properties of superposition and entanglement and their role in enhancing pattern recognition. Although, their work explored the domain of cybersecurity specifically, it lacked experimental benchmarking on large-scale or real-world datasets. Dornala and Senthilkumar [14] proposed a framework, consisting of a combination of behavioral analysis along with graph neural networks and QML, addressing intelligent firewall-based malware detection. The primary focus of their work was architectural improvements, and their framework achieved significant improvements in detection accuracy. However, it lacked a systematic comparison of algorithms based on quantum and classical methods, along with their degree of applicability on various fields of cybersecurity. Eze et al. [15] explored the detection of malicious URLs. They aimed to analyze and compare the performance of classical and quantum-based approaches. In their study, they conclude that quantum approaches, namely QSVMs and quantum convolutional neural networks (QCNNs), outperform classical machine learning methods in classification accuracy. However, their study was limited to a single cybersecurity use case and could not explore the domain of cybersecurity as a whole, with its various subdomains and generalizability across them. Their study also lacked the consideration of systems that employ both classical and quantum approaches in a hybrid manner. Table 1 presents a comparison of this survey with the existing related surveys.

To address these shortcomings, this review presents a unified and comprehensive study of the application of QML in the domain of cybersecurity. This review aims to analyze previous works across diverse threat landscapes, including intrusion detection, malware analysis, quantum federated learning, privacy-preserving encryption, and cloud security, and critically examine both infrastructural and algorithmic perspectives. This paper presents a systematic consolidation of existing techniques, such as QSVM, QNN, QCNN, QGAN, and hybrid quantum–classical models, with a structured taxonomy while also identifying practical gaps, challenges in scalability, interpretability, and hardware dependence.

Novelty of this survey: Unlike recent surveys that either focus on general quantum machine learning (QML) principles or specific cybersecurity applications, this work provides a unified taxonomy that systematically maps QML techniques (e.g., QSVMs, QNNs, VQCs, QGANs) to diverse cybersecurity domains. Additionally, this survey uniquely integrates system-level perspectives, including hybrid quantum–classical architectures, deployment considerations, and evaluation methodologies, while explicitly analyzing practical limitations such as NISQ constraints, scalability challenges, and real-world applicability. This distinguishes our work from prior studies that lack cross-domain synthesis and deployment-focused analysis.

Literature selection methodology: This survey follows a structured approach for literature selection to ensure transparency and

TABLE 1 | Comparison of related surveys on quantum machine learning (QML) in cybersecurity.

References	Primary focus	Key contributions	Limitations	Hybrid	Tax.	Apps.	Bench.
[12]	ML applications of Quantum Computing	Systematic survey of 32 studies integrating QC with ML; covers QSVM, QNN, QCNN, and hybrid learning frameworks	Broad and theoretical; limited domain-specific focus on cybersecurity or benchmark analysis	×	○	○	×
[15]	QML for Malicious URL Detection	Comparative study of QSVM/QCNN vs. SVM/CNN on phishing and URL datasets; highlights early QML feasibility	Single-task focus; lacks scalability, taxonomy, and broader cybersecurity coverage	×	×	○	✓
[13]	QML for Cybersecurity Audits	Explores QNN, QSVM, and QPCA for anomaly detection; conceptual hybrid designs	Theoretical orientation; lacks real-world validation and cross-domain integration	✓	○	×	×
[14]	Intelligent Firewall with QML	Hybrid behavioral analysis + QML + GNNs; improved malware detection	Application-specific; limited taxonomy and inconsistent evaluation	✓	×	✓	✓
Our paper	Comprehensive review of QML for cybersecurity	Taxonomy of QML (QSVM, QNN, QCNN, QGAN); hybrid models; privacy, interpretability, scalability; cross-domain synthesis	Empirical deployments left for future work	✓	✓	✓	✓

Note: ✓ = fully addressed; ○ = partially addressed; × = not addressed. Hybrid = inclusion of hybrid quantum–classical models; Tax. = presence of structured taxonomy; Apps. = application diversity across cybersecurity domains; Bench. = benchmarking or experimental validation.

reproducibility. We queried major academic databases including IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and arXiv. The search was limited to publications from 2018 to 2025 using keywords such as QML, QML cybersecurity, quantum intrusion detection, and quantum anomaly detection. Inclusion criteria consisted of: (i) peer-reviewed articles or high-quality preprints, (ii) works proposing or evaluating QML techniques, and (iii) studies relevant to cybersecurity applications. Exclusion criteria included purely theoretical works without relevance to security, duplicate studies, and articles lacking sufficient experimental or methodological detail. A total of 96 papers were initially identified, out of which 44 were selected after screening titles, abstracts, and full texts.

3 | An Overview of Quantum ML and Cybersecurity

3.1 | Preliminaries of Quantum Computing

Classical bits take a definite value of 0 or 1. A qubit, by contrast, exists in a superposition $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$, and $|\alpha|^2 + |\beta|^2 = 1$. Measurement collapses this state, returning 0 with probability $|\alpha|^2$ and 1 with probability $|\beta|^2$. When multiple qubits are combined, they can become *entangled*: the joint state cannot be factored into independent single-qubit states, so measuring one qubit instantaneously constrains the outcome of another, regardless of distance. Superposition and entanglement together allow an n-qubit register to represent a combination of 2^n basis states simultaneously, which underlies the parallelism exploited by QML algorithms. Quantum computation proceeds by applying *quantum gates*—unitary operations such as the Hadamard gate (creates superposition), Pauli-X/Y/Z gates (bit/phase flips), and controlled gates such as CNOT (creates entanglement)—to qubits, arranged as a *quantum circuit*. In QML, classical data is first mapped into quantum states through a *feature map* $U_\phi(x)$, using strategies such as basis encoding (each classical bit maps to a qubit basis state), angle encoding (features are encoded as rotation angles), amplitude encoding (features are encoded as state amplitudes, allowing exponential compression), or more expressive maps such as the instantaneous quantum polynomial (IQP) or ZZ feature map, which use entangling layers to create feature spaces that are difficult to reproduce with classical kernels. A trainable circuit U_θ (an ansatz) is then applied, and its parameters are optimized—typically via gradient-based methods using the parameter-shift rule, or gradient-free optimizers such as COBYLA—to minimize a task loss [16].

Present-day quantum hardware operates in the *Noisy Intermediate-Scale Quantum (NISQ)* era: devices with tens to a few hundred qubits, no full error correction, and limited coherence times, meaning gate errors and decoherence accumulate quickly with circuit depth. This motivates the shallow-depth, hybrid quantum–classical designs that dominate the QML-for-cybersecurity literature surveyed in this paper, where the quantum processor handles feature encoding or kernel estimation while classical hardware manages preprocessing, optimization, and postprocessing.

3.2 | Quantum ML

QML combines quantum computation with classic statistical learning. It can deliver high-dimensional inference and optimization under strict time and resource budgets. It doesn't propose entirely novel pipelines. Rather, QML involves augmenting existing pipelines using quantum states to represent and transform data through parameterized unitaries that use superposition and entanglement. The representations generated by QML can lead to learning procedures difficult to emulate using traditional methods under specific assumptions about data structure and access models.

In practical applications, QML is generally coupled with classical methods in a hybrid quantum–classical design. Steps like data preprocessing, batching, and optimiser updates are offloaded to classical methods, whereas the quantum processor implements a feature map $U_\phi(x)$ and a trainable circuit U_θ (e.g., a variational quantum circuit). Training involves minimizing a task loss through gradient-based or gradient-free methods, using estimators such as parameter-shift rules [17, 18]. Some alternate formulations also exist, such as quantum kernel methods (e.g., QSVM with implicit kernels induced by U_ϕ) and probabilistic models based on quantum generative circuits. The robustness and trainability are determined by various design parameters, such as the encoding strategy (basis, angle, amplitude), the depth of the circuit, the entangling topology, and the readout observables [19, 20].

Quantum hardware mechanics and machine learning enhance each other in a feedback loop. In machine learning, processes like feature embedding, kernel estimation, or sampling get accelerated by quantum hardware. This enhanced state of machine learning offers better error-correction, control, and calibration. This, in turn, contributes to the stabilization of NISQ hardware. The stabilised NISQ hardware again helps to improve the machine learning processes. This enhancement happens iteratively. Thus, in other words, better hardware improves the model, and the improved models perform better in removing noise and hardware constraints.

QML can be used across various domains, including, but not limited to, artificial intelligence, healthcare, finance, chemistry, materials science, cybersecurity, and climate modeling. It can be used for its abilities in faster computation and data analysis. It can also recognize complex patterns especially well. QML also has a specific use for simulation and combinatorial optimization. In this work, the focus is on the use of QML in the domains of cybersecurity and security analytics. QML offers fast optimizations, and leads to rich feature maps that significantly benefit the domain of cybersecurity. Also, QML can perform similarity evaluations very fast, making it especially suited for detecting anomalies or rare events, and thus staying robust in looking for changes in data patterns. Although, the current state of QML is immature, ongoing advancements in quantum hardware capacity, qubit stability, and software toolchains have led to QML being increasingly competitive in a wider scope of domains.

3.3 | Cybersecurity

Cybersecurity is a crucial domain for managing assets in digital infrastructure. In digital systems such as networks, cloud services, and IoT, assets are interconnected, and a compromise in one component can easily spread to the entire system. Cybersecurity ensures the confidentiality, integrity, and availability of these digital resources. In recent years, the scale of operations and data has expanded substantially. There is now a wide variety of sources of telemetry data, including network traffic, user authentication logs, and endpoint data. Processing such high amounts of diverse and real-time data efficiently becomes a challenging task. The data must be processed with low latency in a privacy-preserving manner, all within the limited computing resources available in real-world scenarios, defense against cyber attacks is not static. It is a battle against continuously evolving intelligent adversaries. Fixed defenses become obsolete as adversaries evolve their attack tactics and techniques, making reactive or signature-based approaches inadequate in such a nonstationary threat landscape. There is a need for security techniques that are proactive and anticipate the evolving nature of attacks and their tactics. Approaches that detect, predict, and respond before the attack causes harm, and provide early threat localization, attack containment, and resilience, are a must. These challenges motivate the development of adaptive, learning-based, and automated defense systems [8, 21].

A robust cybersecurity system is evaluated not just by its accuracy, but also by its ability to detect and contain threats in a timely manner. Time-to-detect (TTD) and time-to-contain (TTC) are key indicators of performance. The system should also be able to handle unseen attack types and the tampering of inputs done by adversarial manipulations. Such a system must also keep false positives extremely low to avoid alert fatigue, while preserving privacy. Thus, we examine systems combining the quantum and classical techniques for cybersecurity. In complex or noisy datasets, the signals are weak [22]. In industrial IoT environments, certificate-based aggregate-signature mechanisms can provide authentication and message integrity while reducing the communication and verification overhead associated with validating large numbers of device messages [23].

4 | How Does QML Enhance Cybersecurity?

Quantum computing leverages parallelism, enabling QML to compute rich similarity measures and sample complex distributions with great efficiency. This happens by encoding telemetry or features into quantum states (via quantum feature maps) and exploiting superposition and entanglement. When the data is high-dimensional and heterogeneous, this use of parallelism can lead to shorter training cycles. These advantages mean the QML is significantly more robust against complex and evasive threats, such as zero-day attacks and APTs, which conceal their activity and continually evolve to evade detection. Due to the above-mentioned advantages such as parallelism, quantum models can process large volumes of telemetry (network flows, system logs, endpoint traces) at scale, thus offering real-time identification of subtle or emerging anomalies and novel attack signatures. For example, even when adversaries camouflage their behavior, QML classifiers can differentiate normal network fluctuations from early-stage intrusions using flow-level features.

QML is not limited to detection. It can provide proactive and reactive defenses that are adaptive and resilient. Using QML, defensive policies can be dynamically updated in real time, accounting for concept drift (changes in normal behavior) and shifting adversarial tactics. Furthermore, quantum generative models can create high-fidelity attack simulations for red-team exercises and what-if analyzes. Being both adaptive and generative in its capabilities, QML can support closed-loop operations across cloud, edge, and on-premise deployments. These automated security deployments result in lower TTD and TTC and fewer false positives due to the rich feature representations of QML. QML also contributes to the modernization of cryptography and security. Post-quantum cryptography (PQC) targets encryption and key management layers, but it can still benefit from QML [24]. PQC protects data at rest and in transit from quantum-capable adversaries, whereas QML strengthens live, real-time network defenses through detection and prioritization. Combined, they ensure both data preservation (via PQC) and operational resilience (via QML) under practical constraints such as latency, energy, or compute limits. Thus, QML's benefit extends beyond reactive defense, providing proactive, learning-driven security. Security provided by QML can scale with increasing data volume and complexity of adversarial attacks. Quantum feature mapping can amplify and detect such weak signals. QML can compute similarity evaluations and distances quickly and efficiently. It can detect anomalies in encrypted traffic without decrypting them by using the pattern in metadata or ciphertext. It can also generate synthetic attack traces, making it useful for red-team training and simulation of hypothetical scenarios.

QML helps in security operations centre (SOC) workflows by improving detection accuracy. It also improves the system's immunity against zero-day attacks. Hybrid QML setups, which combine quantum and classical methods at various stages of the pipeline, can be used to optimise computation, energy, and privacy constraints, which is crucial for operational environments. While, QML offers theoretical advantages such as exponential feature space representation and faster kernel evaluations, empirical validation remains limited. Many studies report improvements in controlled environments or simulations; however, consistent superiority over classical ML in real-world cybersecurity settings is not yet firmly established. Therefore, claims of advantage should be interpreted cautiously, distinguishing between theoretical potential and experimentally verified performance gains.

Table 2 compares classical and QML approaches in their respective strengths and limitations. It also describes what each of these implies for cybersecurity applications.

5 | Applications

The applications of QML in the domain of cybersecurity are multifarious, such as adversarial detection and defense, healthcare data security, malware and botnet identification, and telecommunication protection. Every domain presents unique challenges. Due to the growing complexity of digital infrastructures along with the rapid evolution of cyber threats, traditional machine learning and rule-based systems have been pushed to their limits.

TABLE 2 | Comparison of classical vs. quantum machine learning systems in cybersecurity.

Aspect	Classical ML systems	Quantum ML systems
Threat detection approach	Mostly reactive, identifies and responds after anomalies occur [8].	Proactive: predicts, identifies, and neutralises threats before impact [25].
Cryptographic capabilities	Uses standard encryption, vulnerable to quantum attacks.	Supports quantum-safe encryption and adaptive quantum-secure models [26].
Computational power	Limited by classical hardware, struggles with high-dimensional problems.	Uses quantum parallelism for large-scale optimization and complex datasets [19].
Pattern recognition	Effective for known threats, may miss subtle anomalies.	Detects hidden correlations, identifies zero-day and APT-level threats [27, 28].
Scalability	Performance declines with increasing data complexity.	Quantum-enhanced scaling supports large, dynamic digital ecosystems [26].
Application domains	Used for IDS, malware detection, and threat monitoring [8].	Extends to cybersecurity, finance, healthcare, and climate modeling [19, 26].

In each of these domains, QML models such as QSVMs, QNNs, VQCs, and QGANs, have shown to be much faster, efficient, and robust as compared to their classical counterparts. In the following subsections, we present a detailed survey of these applications and show how QML contributes to future-ready and resilient security frameworks. Figure 1 represents the taxonomy of the applications of QML in cybersecurity.

5.1 | Threat Detection

Classical and conventional detection systems fail to keep pace with the exceedingly complex cyber threats. Rule-based defenses, and in many cases, even classical machine learning models, are misled by modern-day attacks such as zero-day exploits, polymorphic malware, and APTs, which are deliberately engineered to bypass these approaches. These approaches are also limited by computational overhead, where they lack the required acceleration to process the scale of computations. They also lack the flexibility needed to track evolving attack vectors. QML is heavily accelerated due to its use of quantum computations, which also enables rapid model updates, allowing for real-time anomaly detection and policy-driven responses. All these properties make QML-based approaches much more durable and better aligned with future threat dynamics [29].

To test the potential of QML-driven intrusion detection at a large scale, and both known and zero-day attacks, Awasthi [3] tested and reported high detection rates on evaluated workloads. They leveraged quantum parallelism to evaluate large sets of attack patterns simultaneously. The system used quantum-enhanced feature analysis and processed incoming network events. Thus, the system was capable of examining up to 2^{20} potential attack vectors in parallel. They benchmarked it against classical IDS systems for comparison. Their methodology involved measuring detection accuracy, latency, and false-positive rates across known and zero-day attack scenarios under identical conditions. Thus, they were able to perform a direct performance assessment between quantum and classical approaches. They found a 96.4% detection rate for zero-day attacks and 99.7% for the known ones. The false positive rate also was just 0.03%. These results indicate potential for real-time detection and response at enterprise scale.

TABLE 3 | Comparison of threat detection studies.

Study	Method	Reported result
Awasthi [3]	Quantum-parallel IDS (2^{20} vectors)	96.4% (zero-day), 99.7% (known), 0.03% FPR
Karamchand et al. [30]	QSVM + VQC hybrid	QSVM beat classical SVM; VQC more sensitive to faint anomalies

Karamchand [30] proposed a mixed approach of quantum and classical detection in their framework targeting high-security deployments. In their approach, classical pre-processing was used to transform inputs into a high-dimensional feature space in which weak threat patterns become more distinguishable. The transformed inputs were then fed into quantum-based classifiers such as QSVMs and VQCs for classification and clustering. Their evaluation on concealed threats showed that QSVMs were able to outperform their classical counterpart. Also, VQCs showed much better sensitivity to faint behavioral anomalies than what standard neural networks were able to achieve. These findings demonstrate the accuracy gains and enhanced anomaly awareness that QML models can provide in high-risk cybersecurity environments. Table 3summarizes the accuracy and methodological differences across the threat detection studies discussed above.

5.2 | Data Handling and Privacy

In modern cybersecurity, the secure management of data is a core component, particularly in domains that handle high-value and sensitive data, such as healthcare and communication systems. QML can secure health records, encrypted communication channels, and other confidential datasets against evolving cyber threats by using quantum-enhanced encryption methods. QML can also utilise privacy-preserving learning methods, such as federated or encrypted learning, ensuring that the training process can occur without exposing the raw data. It can make data handling systems trustworthy and reliable by using these quantum-enhanced encryption techniques and

privacy-preserving learning models [31–33]. In smart healthcare, federated-learning architectures can support collaborative intelligent diagnosis while retaining patient data locally. Blockchain- or NFT-supported sharing mechanisms can further provide traceability, access control, and accountable exchange of medical information [34]. The integration of blockchain and artificial intelligence has been explored as a means of supporting secure, scalable, traceable, and decentralized healthcare analytics. Blockchain can provide tamper-resistant and auditable data management, while AI supports intelligent diagnosis and processing of healthcare information [35]. These complementary security mechanisms may also support future QML healthcare pipelines by strengthening data provenance and access accountability.

Gupta et al. [8] proposed IQ-HDM, an intelligent quantum cybersecurity framework for healthcare data management. The aim of their proposed framework was to create an environment for managing healthcare data that is both secure and efficient. The proposed IQ-HDM framework comprises two modules: Quantum one-time padding encryption (QOTPE) and quantum feed-forward neural network (QFNN). QOTPE handled secure data storage by encrypting healthcare data into maximally mixed quantum states, while QFNN handled the detection of malicious intent and abnormal behavior. This ensured that the data remains confidential while providing robust analysis of user behavior patterns, allowing the framework to identify threats proactively and prevent incidents before damage occurs. The proposed framework achieved 89.02% accuracy, significantly outperforming classical baselines by up to 67.6% in performance. Paper [36] bridges quantum-adjacent encryption with medical IoT security [37].

A recent study [38] focused on cybersecurity for healthcare systems, where sensitive patient data demands strict protection. This study examined how QML can be integrated with human-factor awareness to develop analytics pipelines that are more secure and trustworthy. In their framework, a local differential privacy (LDP) mechanism is applied before any training occurs. This layer adds controlled noise or perturbation to the raw data, ensuring that individual patient records remain private even if compromised. This privacy preprocessing happens before the quantum learning stage begins, forming the first shield of defense. Then, the quantum random forest (QRF) algorithm is used for secure pattern learning, enabling robust classification on large, high-dimensional datasets. Their approach proved to offer both speed and accuracy improvements compared to classical models, as the framework reached 99.9% detection accuracy on the WUSTL EHMS 2020 dataset and 98.57% on the ICU dataset. The privacy layer did not degrade performance, proving that strong privacy guarantees and high detection accuracy can coexist. Their study demonstrates QML's ability to maintain high detection accuracy while preserving data confidentiality in electronic healthcare systems. Table 4 compares the accuracy achieved by the privacy-preserving QML frameworks discussed in this subsection.

TABLE 4 | Comparison of data handling and privacy studies.

Study	Method	Accuracy
Gupta et al. [8]	QOTPE + QFNN (IQ-HDM)	89.02% (up to 67.6% gain over classical)
(Study) [38]	LDP + quantum random forest	99.9% (WUSTL EHMS 2020), 98.57% (ICU)

5.3 | DGA Botnet Detection

Domain generation algorithm (DGA) botnets create a large number of pseudo-random domain names to communicate with their command-and-control servers. Classical detection systems and blacklist-based methods struggle to effectively detect or block such domains. QML offers alternative mechanisms, which are able to recognise these dynamic and complex domain generation patterns, and thus QML-based detection improves both the speed and reliability of identifying DGA-driven botnet activities.

In NISQ hardware, quantum noise and limited qubit counts constrain performance. Tehrani [27] examined hybrid learning approaches that combine quantum and classical methods to evaluate their effectiveness under these constraints for cybersecurity applications. The researchers used a combination of real quantum processors and simulators, including those from IonQ, Rigetti, and Continuum, along with the IBM AER simulator, and carried out experiments on the DGA Botnet dataset to evaluate intrusion and botnet detection. They compared several quantum and hybrid algorithms, such as QNNs, QSVCs, Pegasus classifiers, and VQCs, and also proposed a novel algorithm called the quantum Hoeffding tree classifier (QHTC). QHTC outperformed all other models in terms of accuracy and speed while avoiding the optimization issues common in variational circuit models. These results indicate significant gains from quantum-enhanced models, even when the hardware remains noisy and of small scale. Their study confirmed that, in real-world NISQ environments, models like QHTC are practical and secure for botnet and intrusion detection tasks.

Suryotrisongko and Musashi [9] developed a hybrid deep learning framework combining quantum and classical components to detect botnet activity generated by domain-generating algorithms. Botnets created through such algorithms are particularly difficult to identify. The framework incorporated quantum feature encoding techniques using PennyLane angle embeddings and IQP embeddings, which enabled the mapping of classical features into quantum state representations. The authors experimented with multiple circuit architectures, including basic entangler layers, random quantum layers, and strongly entangling layers. The hybrid model achieved up to 94.7% accuracy, significantly outperforming classical baselines. They concluded that quantum-enhanced embeddings and circuit designs are especially effective for botnet detection and broader cybersecurity analytics. Tehrani et al. [39] used a QHTC for detecting DGA botnets. They employed a hybrid approach that utilised both quantum and classical methods to enhance the accuracy and efficiency of real-time detection in network environments. They used public cloud infrastructure such as Google Cloud and Microsoft Azure, along with quantum providers like Rigetti, IonQ, and Quantinuum. The IBM Qiskit framework and AER simulator were used for quantum circuit design and experimentation. They found that the model achieved a perfect accuracy of 100% in the final testing run. Across 5000 test samples, it reached an average accuracy

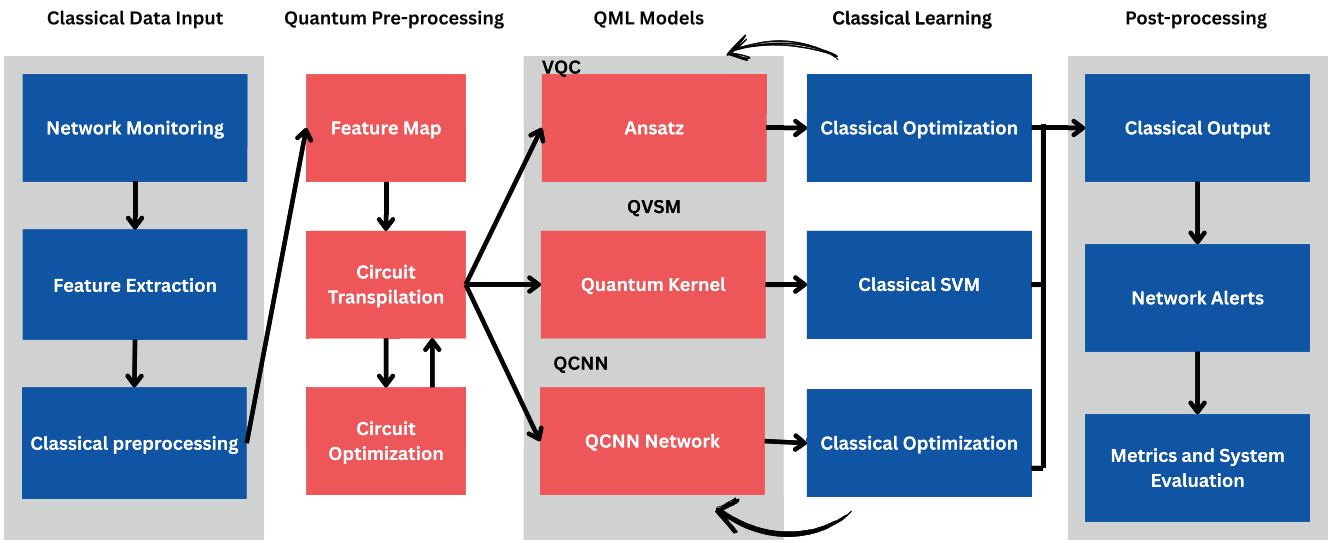

FIGURE 2 | Operational flowchart of QML-IDS showing end-to-end integration of classical and quantum components, including network monitoring, quantum circuit optimization, QML model execution (VQC, QSVM, QCNN), and classical post-processing for threat detection and evaluation.

TABLE 5 | Comparison of DGA botnet detection studies.

Study	Method	Accuracy/result
Tehrani [27]	QHTC vs. QNN, QSVC, Pegasos, VQC	QHTC best overall (IonQ, Rigetti, Continuum, IBM AER)
Suryotrisongko and Musashi [9]	Angle/IQP embeddings	94.7%
Tehrani et al. [39]	QHTC (cloud deployment)	100% final run, 91.2% avg over 5000 samples, 1687 s
Abreu et al. [40]	VQC, QSVM, QCNN (QML-IDS)	F1 95.60% (CIC-IDS-17, binary), 98.88% (UNSW-NB15, multiclass)

of 91.2%, completing the entire process in just 1687 s. Previous experiments had been limited to simulated runs only, where accuracy plateaued at around 76.8% on a smaller dataset of 1000 samples. Thus, a substantial gain in performance and scalability is indicated when moving from simulation-only setups to real hybrid cloud deployments. These results validate the feasibility of integrating quantum-enhanced classifiers with cloud-based cybersecurity systems.

Abreu et al. [40] introduced QML-IDS, combining classical methods with multiple quantum models such as VQCs, QSVMs, and QCNNs for enhanced intrusion detection. They evaluated the framework on IBM Kyoto and IBM Osaka NISQ hardware backends. They found that QML-IDS was able to outperform classical baselines in both binary and multiclass classification. The QCNN model achieved a high F1-score of 95.60% on the CIC-IDS-17 dataset for binary classification and 98.88% for multiclass analysis attack classification on the UNSW-NB-15 dataset. Although, they were not able to significantly outperform classical methods in all aspects, they were equal to or superior to traditional methods. Figure 2 shows the working of the QML-IDS system. Table 5 summarizes the methods and reported accuracy of the DGA botnet detection studies surveyed above.

5.4 | Malware

QML has been recently explored in the domain of malware detection and containment. Malware evolves rapidly, and QML can offer adaptive detection, improving detection accuracy that traditional static systems are unable to achieve [41]. Bikku et al. [42] proposed a QNN-based framework for detecting malware was proposed. It consisted of three phases: feature extraction, classification, and real-time analysis, all of which were achieved through quantum methods. Quantum-based feature extraction was used to capture malware characteristics, and then a QNN was used for differentiating between malicious and benign samples. This framework was tested on the MalwareDB dataset, and it achieved 95% accuracy, not only outperforming the classical machine learning models such as support vector machines (SVMs) and Random Forests, but quantum baselines such as quantum SVMs and quantum decision trees, all while having a minimal latency.

Barrué and Quertier [43] analyzed several classical algorithms with their quantum counterparts, for generalizable and robust malware detection. They compared QSVMs and QNNs with classical SVMs and neural networks. They tested two different preprocessing approaches. In the first approach, they performed executable-to-image transformation, converting binary executables into image representations. In the second approach, they used ordered importance features (OIF) extraction, focusing on statistics across different attributes. They achieved 80.75% accuracy using a QSVM with the $ZZphiFeatureMap$ on the image-based dataset, outperforming classical SVMs, which achieved 77% accuracy with linear and polynomial kernels. On the OIF dataset, the QSVM with the $ZZpFeatureMap$ reached 95% accuracy, comparable to the best classical SVMs. QNNs could not outperform classical models in accuracy, but optimization methods such as Simultaneous Perturbation Stochastic Bifurcation and data re-uploading improved runtime efficiency on the same accuracy.

In Krátká et al. [44] the performance of classical SVMs were compared with QSVMs for binary malware detection. The

TABLE 6 | Comparison of malware detection studies.

Study	Method	Accuracy/notes
Bikku et al. [42]	QNN (3-phase pipeline)	95%; beat classical SVM/RF and quantum SVM/decision-tree baselines; low latency
Barrué and Quertier [43]	QSVM (ZZFeatureMap) vs. classical SVM	80.75% (image-based) vs. 77% classical; 95% (OIF-based), comparable to best classical SVM
Barrué and Quertier [43]	QNN + SPSB, data re-uploading	Did not beat classical accuracy; improved runtime at same accuracy
Krátká et al. [44]	QSVM vs. classical SVM	Performance gain noted; higher compute time from circuit transpilation, job-size limits

experiments showed the performance boost achieved in the quantum-based approach over the classical approach, but also highlighted some challenges experienced in the former. Computation time was increased due to circuit transpilation, and job size limitations on quantum hardware meant that these experiments could not be performed on a large scale. Also, the current evaluation infrastructure lacked the efficiency and compatibility to run these experiments on scale. The study concluded that QSVM-based approaches are bound to become increasingly practical and applicable for real-world malware detection tasks as hardware and software quantum infrastructure evolves. Table 6 presents a comparative summary of the malware detection studies discussed in this subsection.

5.5 | Anomaly Detection

In the context of cybersecurity, an anomaly refers to unusual or suspicious patterns that may indicate malicious activity. Anomaly detection involves the use of detection techniques to accurately identify such patterns. QML has resulted in novel approaches that enhance both accuracy and efficiency beyond what classical detection techniques can achieve. This advantage stems from QML's ability to model non-linear and high-dimensional patterns. In this subsection, a review is provided for recent advancements in QML-based anomaly detection methods. This subsection also highlights their practical applications in cybersecurity [21].

With their advent, QML models have shown impressive performance in terms of accuracy and latency. Hossain et al. [2] integrated QNNs and QSVMs in a hybrid pipeline for real-time monitoring of network traffic. The QNN achieved 96% accuracy in anomaly detection, and the QSVM achieved 93% accuracy, with the average alerting latency being near-instant at 10 ms. Exploring further, Noah et al. [45] ventured in QML for cybersecurity in 5G networks. They used hybrid simulations using the IBM Qiskit and TensorFlow Quantum frameworks. Their quantum-assisted intrusion detection system, based on QNNs, achieved 96.8% accuracy, whereas the classical approaches scored only achieved only 92.3%. Their QSVM was able to achieve an F1 score of 0.94 for zero-day attack detection, whereas classical models achieved just 0.87%. Also, the detection latency got reduced from 320 to 110 ms with quantum processing, which is a critical improvement in this domain. Still, the authors noted that hardware noise and limitations, interoperability issues, and cost remain hindrances to the adoption of this technology.

TABLE 7 | Comparison of anomaly detection studies.

Study	Method	Accuracy/latency
Hossain et al. [2]	QNN + QSVM hybrid	96%/93%, ~10 ms alerting latency
Noah et al. [45]	QNN, QSVM (5G, Qiskit + TFQ)	96.8% vs. 92.3% classical; F1 0.94 vs. 0.87; latency 320→110 ms

Quantum hardware is not used only in defense, but also as an offensive weapon. Thus, QML is instrumental in not just safeguarding against classical threats, but quantum-enhanced ones. In their work, Oyebode and Jimoh [28] report that as quantum hardware advances, QML is expected to become central to securing telecommunication infrastructures against both classical and quantum-enabled threats. QML can use quantum parallelism and entanglement to process large datasets more efficiently. The paper discussed cybersecurity applications, including quantum-enhanced anomaly detection using quantum kernels and QSVMs for analyzing encrypted traffic. They also discussed emerging approaches that integrate QNNs with classical deep learning in hybrid architectures. Table 7 compares the accuracy and latency figures reported by the anomaly detection studies above.

5.6 | Adversarial Attacks

Robust detection frameworks are crucial against adversarial attacks that are gradient-free. In their work, Kejriwal et al. [46] proposed a quantum-based defense framework for defense against such attacks, combining classical components with QSVMs based on quantum kernels. They evaluated the framework on a combination of malware detection and network intrusion datasets. In their analysis, classical deep models suffered more than 85% attack success, while the quantum-based methods reduced the vulnerability by up to 60%. Similarly, Ergu et al. [47] explored 6G interference classification by integrating QML with Open Radio Access Network architectures. They proposed a Hybrid Quantum–Classical Neural Network (HQ-CNN). They used ResNet-18 for deep feature extraction and Principal Component Analysis for dimensionality reduction. By using Q-Poison attacks, they manipulate network state classifications. Their HQCNN was able to achieve an accuracy of 78.5% on clean data, but sees a 1.44× drop to just 54.6% when fed with the attacks. Thus, defenses against adversarial threats that exploit quantum coherence need to be strengthened further [48].

Figure 3 illustrates the range of QML applications in cybersecurity.

While individual studies report promising performance gains, a direct comparison across QML techniques reveals important trade-offs. QSVM-based methods consistently demonstrate

FIGURE 3 | Application landscape of quantum machine learning in cybersecurity.

strong performance in structured datasets (e.g., intrusion detection, malware classification) due to their effective quantum kernel mappings, but they are sensitive to feature encoding strategies and kernel design. In contrast, QNNs and VQCs provide greater flexibility and adaptability to dynamic threat environments, such as zero-day attacks and adversarial settings, but suffer from optimization instability and higher training complexity. Hybrid quantum–classical models emerge as the most practical approach in current NISQ settings, combining classical preprocessing with quantum feature transformations to balance scalability and performance. Notably, across applications such as DGA detection, anomaly detection, and malware analysis, improvements reported by QML models are often dataset-dependent and achieved under controlled conditions. This highlights that while QML demonstrates potential advantages in high-dimensional pattern recognition, consistent superiority over classical methods in real-world cybersecurity pipelines remains an open challenge. Furthermore, generative approaches such as QGANs provide unique capabilities for adversarial simulation and synthetic attack generation, which are not easily replicated by classical models. However, their stability and training efficiency remain limited. Overall, the comparative analysis suggests that no single QML technique universally outperforms others; instead, their effectiveness depends on the application domain, data characteristics, and hardware constraints.

Table 8 summarizes the datasets used in above mentioned studies. Table 9 summarizes the defense methods and reported robustness gains from the adversarial attack studies discussed in this subsection.

TABLE 8 | Summary of datasets and evaluation metrics in surveyed QML studies.

Study	Dataset	Task	Metrics
[40]	CIC-IDS-17, UNSW-NB15	Intrusion detection	Accuracy, F1-score
[39]	DGA botnet dataset	Botnet detection	Accuracy, runtime
[8]	Healthcare dataset	Anomaly detection	Accuracy
[45]	5G network data	Intrusion detection	Accuracy, latency, F1-score

TABLE 9 | Comparison of adversarial attack defense studies.

Study	Method	Result
Kejriwal et al. [46]	QSVM (quantum kernels)	Vulnerability reduced up to 60% (vs. 85% + classical attack success)
Ergu et al. [47]	HQCNN (ResNet-18 + PCA)	78.5% clean → 54.6% under Q-Poison (1.44× drop)

6 | ML Techniques-Based Classification

Machine Learning serves as the foundation for both classical and quantum approaches in cybersecurity. ML enables learning

from data, detecting hidden patterns, and adapting to evolving threats. Within QML, these methods are done through quantum mechanics, allowing models to operate in higher-dimensional feature spaces. It allows models to optimise more efficiently, and, in some settings, achieve greater accuracy in classification or clustering tasks. Core ML, including supervised learning, unsupervised learning, and generative modeling, when applied to the quantum domain, result in algorithms such as QSVMs, QNNs, VQCs, Quantum k-Means, and QGANs. Structured attacks are detected well by supervised models, and hidden anomalies in large datasets are detected by unsupervised learning. Generative models can simulate complex and dynamic threat scenarios for adversarial defense. This section highlights such major ML techniques adapted for QML and their applications in cybersecurity.

6.1 | Supervised Learning

Supervised learning has become a key technique for cyber defense, where models trained on labeled attack and benign traffic samples automatically detect and classify diverse threat types. Classical supervised algorithms like Neural Networks and SVMs can achieve strong performance, but their training and inference costs grow rapidly with data volume and feature dimensionality, making scalability difficult. Quantum computing can process high-dimensional, complex threat signatures more efficiently, and explore richer decision boundaries and patterns that may be difficult for classical methods to capture at scale. By combining supervised learning with quantum resources, these models aim to deliver more efficient and accurate threat detection pipelines. This is particularly true in scenarios involving massive, rapidly changing cyber telemetry where classical approaches begin to struggle.

6.1.1 | Quantum Support Vector Machines

QSVMs address a key problem in distinguishing malicious activity from normal behavior. The differences in these activities can be very subtle. QSVMs map data into quantum feature spaces, making patterns easier to identify, while also accelerating computation for enhanced performance [49]. Janak et al. [50] proposed a QSVM-based framework to detect false data injection attacks (FDIAs) in power distribution systems. The model was able to surpass classical SVMs in both accuracy and speed. It could efficiently spot small anomalies within high-dimensional data by quantum feature mapping, which led to an accuracy of 94.67%. It also achieved an AUC of 0.98 for ramp attacks and 0.97 for random attacks on the ROC curve.

Kejriwal et al. [46] demonstrated the ability of QSVMs to provide resilience to adversaries in practical deployments. A hybrid classical–quantum QSVM was used to counter gradient-free adversarial attacks. By leveraging noise-robust quantum kernels, adversarial susceptibility got reduced by 40%–60% on cybersecurity datasets while maintaining strong performance on clean data.

6.1.2 | Quantum Neural Networks

QNNs and QCNNs provide advanced pattern recognition. They have been shown to be especially effective for intrusion detection and malware analysis, which require models that generalise across diverse and dynamic datasets.

Küçükkara et al. [51] built an intrusion detection system using QNNs to classify DDoS attacks. They trained and tested their framework on the CIC-DDoS 2019 dataset. Their architecture utilised quantum parallelism and superposition for faster pattern processing and achieved an accuracy of 92.63%. Bikku et al. [42] designed a QNN-based framework for real-time malware detection. Their architecture had three main stages: quantum feature extraction, classification with a variational quantum circuit, and connection to a real-time analysis pipeline. They evaluated their architecture on the Malware DB dataset and achieved a 95% accuracy, outperforming classical models and other quantum baselines. They achieved all this while maintaining low latency. Thus, they demonstrated that their architecture is suitable for real-time deployment.

6.1.3 | Variational Quantum Classifiers

VQCs combine parameterized quantum circuits with classical optimisers in hybrid feedback loops. Thus, they can adapt to evolving attack strategies. Abreu et al. [40] integrated classical variational algorithms into quantum workflows by encoding classical data into quantum states, processing them with variational circuits, and optimising parameters for improved classification. Tehrani [27] compared several hybrid quantum–classical binary classifiers on a DGA botnet dataset, with a focus on VQCs. They also pitched QHTC as an alternative.

Rahman et al. [52] performed cyberattack detection using VQCs on the NSL-KDD dataset. They reduced the features from 8 to 3 using PCA. Their EfficientSU2 circuit with the COBYLA optimiser achieved 93% training and 90% test accuracy. They were able to beat both classical SVMs and other VQC implementations. Thus, they confirmed that fine-tuned VQCs can deliver strong cybersecurity performance. Figure 4 illustrates the circuits underlying these approaches.

6.2 | Unsupervised Learning (Clustering)

Quantum computing makes clustering faster and more insightful using parallelism and entanglement. Thus, they overcome the limitations of classical unsupervised learning techniques like k-means and PCA, such as scalability and complex high-dimensional data. This is important because cybersecurity logs and network traffic often consist of vast amounts of unlabeled data [53].

6.2.1 | Quantum k-Means Clustering

Quantum k-means uses quantum computation to accelerate distance calculations, and thus they aim to produce more accurate and efficient cluster assignments. Maouaki et al. [54] proposed a framework for QML clustering for cybersecurity vulnerabilities. The dataset they targeted was the 2022 CISA known exploited vulnerabilities (K-EV) catalogue. They used the QCSWAP k-means and QKernel k-means methods and outperformed classical k-means with a Silhouette score of 0.491 and a

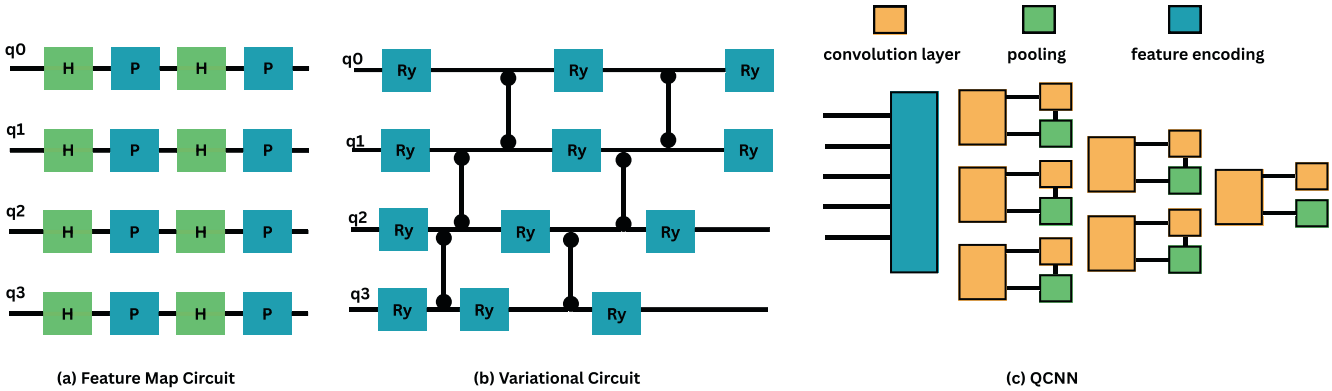

FIGURE 4 | Quantum circuits used in QML: (a) feature-map circuit, (b) variational circuit, and (c) quantum convolutional neural network (QCNN) showing convolution, pooling, and feature encoding.

Davies–Bouldin index below 0.745. They generated more meaningful clusters based on severity levels and affected products.

The QCSWAP k-means method relies on the SWAP test to estimate similarity between quantum states. The SWAP test is a quantum circuit that computes the inner product between two states ψ and ϕ, which corresponds to their similarity or distance. By measuring the probability of the ancillary qubit, the overlap between the two states can be efficiently estimated. This provides a potential quantum advantage, as distance calculations in high-dimensional spaces can be performed with fewer computational resources compared to classical pairwise distance computations. Consequently, clustering algorithms such as quantum k-means can scale more efficiently for large and complex cybersecurity datasets. Similarly, Chen et al. [55] proposed a QALO-K hybrid clustering method combining classical k-means with a quantum-inspired ant lion optimization strategy. They used quantum encoding and revolving gates for enhanced search and convergence and addressed k-means issues such as poor initialization and local minima traps. They thus achieved more than 98% detection accuracy on multiple datasets, including intrusion detection datasets.

6.3 | Generative Adversarial Networks

GANs can be used to generate synthetic attack data for training robust detection models. Quantum GANs use quantum circuits to capture complex distributions better than their classical counterparts. Rahman et al. [56] developed a QGAN using Qiskit for intrusion detection. They achieved a complexity of $O(n)$ and the system enhanced security defenses by identifying malicious packets more effectively than classical methods for generating extraordinary traffic patterns. Cirillo et al. [57] also proposed a hybrid QGAN framework. They only utilised quantum technology in the generator and kept the discriminator block based on classical methods. They evaluated their framework in the NSL-KDD dataset. The model achieved an accuracy of 0.937 and an F1 score of 0.9384. As they repeated the generator blocks and increased the discriminator size, they found improved performance. They indicated that their framework could balance accuracy and realism while maintaining stable training.

Cross-comparative perspective on QML techniques: While the above discussion outlines individual QML techniques across supervised, unsupervised, and generative paradigms [58], a comparative analysis reveals key differences in their effectiveness for cybersecurity tasks. QSVMs demonstrate strong performance in structured classification problems such as intrusion detection and malware analysis, primarily due to their ability to leverage quantum kernel mappings for enhanced feature separation. However, their effectiveness is highly sensitive to the choice of feature encoding and kernel design, limiting robustness across diverse datasets.

In contrast, QNNs and VQCs provide greater flexibility and adaptability in dynamic threat environments, including zero-day attacks and adversarial settings, owing to their parameterized and trainable circuit architectures. Despite this, they often suffer from optimization challenges such as barren plateaus, training instability, and increased computational overhead, which can hinder scalability in real-world deployments.

For unsupervised learning, quantum clustering approaches such as QCSWAP k-means offer advantages in similarity estimation through quantum state overlap, enabling more efficient handling of high-dimensional and unlabeled cybersecurity data. However, these benefits remain constrained by current NISQ hardware limitations and noise sensitivity. Generative models such as QGANs introduce unique capabilities for simulating adversarial scenarios and generating synthetic attack data, which are valuable for robustness evaluation and training. Nevertheless, their convergence stability and training efficiency are still less mature compared to classical generative models.

Overall, no single QML technique consistently outperforms others across all cybersecurity applications. Their effectiveness is highly context-dependent, influenced by factors such as data characteristics, encoding strategies, circuit depth, and hardware constraints. This highlights the importance of hybrid quantum–classical approaches, which currently provide the most practical balance between performance, scalability, and deployment feasibility in cybersecurity systems.

7 | QML for Cloud Computing Security

Cloud computing centralizes massive data and services on shared, virtualised infrastructure, creating risks like data

breaches, insecure APIs, misconfigurations, and insider threats. This introduces complex and dynamic security challenges. As adversaries begin to explore quantum-capable attacks, many conventional cryptographic and defensive mechanisms are expected to become fragile or obsolete. Thus, there is a need to move beyond purely classical cybersecurity strategies. This threat landscape has inspired interest in defenses that are quantum-enhanced and can withstand both current and future adversarial tactics, including those equipped with scalable quantum hardware. Recent works have investigated how QML and other quantum technologies can be embedded into cloud-based infrastructures to enable more proactive, adaptive, and scalable security services, rather than relying on static or ad hoc protections. These studies suggest that quantum-enhanced security models can overcome several key limitations of classical techniques, offering stronger protection for sensitive data [59].

Zeng et al. [60] proposed a secure framework for quantum federated learning using third-party quantum servers that allow classical users to participate. They used Quantum Homomorphic Encryption as the core mechanism, enabling computation on encrypted quantum data, therefore, preserving the contents, not revealing them. The framework introduced the quantum circuit random reconstruction homomorphic encryption algorithm (QCRRA). This algorithm encrypts variational circuits locally before sending them to the remote quantum server. This way, they protect both the user data and the structure of the model itself. They evaluated on a binary classification task using ad hoc, MNIST and, CIFAR-10 datasets. Their encrypted model, referred to as Encrypted Variational Quantum Circuit (En_VQC), achieved an accuracy comparable to that of unencrypted VQCs. In several cases, En_VQC converges faster and reduces communication overhead. Therefore, QCRRA provides a theoretically infinite ciphertext space, providing much better strength and protection against ciphertext-based attacks. Also, their design maintained usability and model performance while ensuring data and model privacy in quantum federated learning [61–63].

Salvakkam et al. [64] introduced EICDL, which stands for ensemble intrusion detection model for cloud computing using deep learning. They designed it to strengthen defenses against quantum-enabled attacks on machine learning systems. Their architecture combines deep learning models with classical machine learning classifiers, thereby increasing both accuracy and reliability compared to stand-alone methods. Their framework was able to achieve improvements in detection precision, efficiency, and ability to identify follow-up attacks. They evaluated it on KDD-CUP-1999, UNSW-NB15, and NSL-KDD datasets. The architecture achieved a recall of 92.14%, outperforming existing intrusion detection baseline models. This analysis showed promise that hybrid deep learning and classical ML architectures can better secure cloud environments.

Gupta et al. [65] presented a QML-based malicious user prediction (QM-MUP) scheme for identifying attackers in cloud environments before they gain access to sensitive data. They use QNNs trained on simulated user behavior patterns, using qubits and quantum gate operations to capture richer, high-dimensional relationships in access and activity profiles than classical models typically can. QM-MUP achieved a 33.28% improvement in overall system security relative to existing prediction approaches. They also achieved consistently high detection accuracy and were able to reliably flag malicious users. Complementing this predictive line of work, Kaliyamoorthy et al. [66] proposed QMLFD-RSA, a cryptosystem designed to strengthen data integrity and security for public cloud storage scenarios. Their scheme combines the quasi-modified Lévy flight distribution (QMLFD) algorithm with the RSA public-key framework. QMLFD was used to improve key or parameter generation, while the RSA role ensured compatibility with existing infrastructures. The authors reported a packet delivery rate of 97.3%, a throughput of 800 kbps, and a time complexity value of 97.3%. Compared with baseline schemes such as RSA and DES, their results indicate that QMLFD-RSA offers significantly reduced time complexity. It also shows strong delivery and throughput characteristics, yielding a more efficient and secure option for cloud data integrity and communication.

Hybrid quantum–classical architectures built on QML have sparked particular interest for cloud management. Researchers claim that these hybrids lower runtime, energy use, and scaling stress compared to classical AI tools in hosted environments. Maddali [67] proposed a framework that tries to push this promise into overcoming latency, inefficiency, and scalability bottlenecks in real-world cloud operations. The model combines quantum kernel methods, quantum Boltzmann machines, and variational quantum circuits within a broader classical framework for governance. The primary focus of their study was on anomaly detection and data consistency checks over cloud-hosted datasets flowing through shared clouds. The authors evaluated their framework on datasets drawn from finance, healthcare, and IoT sectors, and the results indicated up to a 10× speedup in anomaly detection and data quality verification relative to classical AI baselines. Execution times reduced by as much as 80% and performance-conversion overheads cut by roughly 70%, thus supporting the claims of improved speed, energy efficiency, and scalability. Despite these gains, Maddali and other studies remarked that hardware immaturity, deployment costs, and interoperability with existing cloud stacks remain obstacles for large-scale adoption of QML-based governance solutions. Broadly, the literature on QML in cloud security spans secure federated learning [68], quantum-safe and homomorphically encrypted analytics, proactive malicious-user prediction schemes, and quantum-enhanced data integrity and quality frameworks. Across these domains, QML-based approaches frequently outperform classical models on key metrics such as detection accuracy, computational efficiency, and scalability under realistic cloud workloads. These findings suggest that quantum-enhanced cloud security is gradually shifting from largely theoretical proposals to practically viable architectures, laying the groundwork for more secure, intelligent, and resilient cloud infrastructures.

7.1 | Future Potential in Cloud Computing

In cloud settings, QML must move from demonstrations to real services by supporting secure circuit submission usage quotas

and auditable shot budgets. It must also create quantum-native patterns for multi-tenant use with strict isolation. Additionally, QML must provide serverless interfaces for variational inference and kernel execution, with clear latency and support for cross-targets. As far as privacy-preserving learning is concerned, it should combine quantum-predicted learning with PQC and LDP, along with confidential computing [69].

QML for the cloud should have explicit tracking of privacy versus utility data for encrypted data and model updates in regulated sectors. Reliability engineering should include fallback paths to classical circuit detectors, disaster recovery for analytics pipelines, also it should have circuit-level retries and cross-region circuit application. It should also have chaos-testing focused on quantum job queues and contributions. Resource and cost management should have cost models that link spending to incidents prevented, detection made, and service-level goals, with control of batch sizes, repartition counts, and error-mitigation processes. It should also have schedulers that decide optimal placement across simulators and hardware. As far as security is concerned, attestation for encrypted in-use analytics is a must. Also, audit evidence aligned to compliance frameworks should be provided. Integrating IAM, Key Management, SIEM, SOAR tools, and Zero Trust policies would also help in security and compliance requirements.

As far as the edge cloud partnership strategy is concerned, feature extraction and privacy filters must be done at the edge, quantum kernels or variational layers in the cloud. We should measure end-to-end latency and reliability in distributed departments. Feature operability is also must, where standard APIs for data encoding, circuit specs, and telemetry are needed. Also needed is a benchmark source for contemplated security workloads that reports accuracy, latency, throughput, energy, cost, and robustness. A summary of future directions of research discussed above have been provided in Figure 5.

8 | Limitations

While QML is promising for cybersecurity, its deployment in the real world is hindered by several practical and fundamental obstacles. As per current works, the technology is still in a formative stage. This is true for both the quantum hardware as well as the algorithmic frameworks around it, hindering its scalability, dependability and adoption. The testing in operational environments has been very limited. NISQ hardware restrictions and training inefficiencies introduce further complications. Some additional concerns, such as lack of interpretability, high costs, unclear regulatory standards, and the dual-use nature of quantum technologies, have also been raised in the course of shifting from research prototypes to full-scale deployments. These limitations have been discussed in detail in the subsections that follow.

8.1 | Hardware Constraints & NISQ Limitations

While QML shows promise in intrusion detection, anomaly recognition, and malware analysis, it is limited by the current state of NISQ devices. Current machines have limited qubits, are highly susceptible to noise, and have short coherence times. All these factors lead to low circuit stability, low model precision, and undermined threat detection reliability. In the domain of security, these noisy outputs can produce false positives that erode analyst trust. In their systematic mapping study (SMS), Khanal et al. [70] analyzed these challenges for supervised QML, evaluated on widely used datasets such as MNIST and IRIS. They focused on the choice of hardware, datasets, optimization strategies, and generalization.

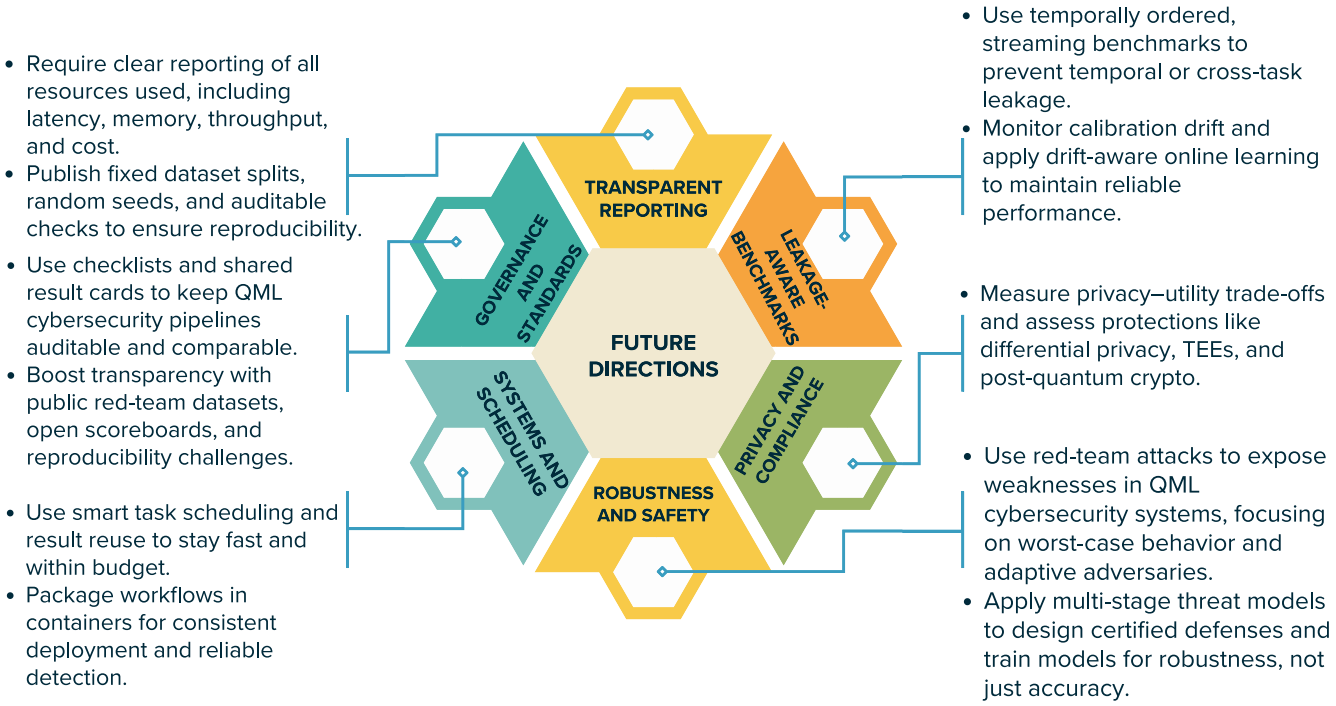

FIGURE 5 | Summary of future research directions.

8.2 | Optimization Challenges & Barren Plateaus

QML models used in cybersecurity, such as QNNs and VQCs, suffer optimization issues. These include barren plateaus, vanishing gradients, and unstable convergence. This limits their scalability and consistency [71]. Suryotrisongko and Musashi [9] and Barrué and Quertier [43] discuss possible solutions such as data re-uploading and sparse parameterisation, but these solutions introduce additional computation, complexity, and reduced interpretability, complicating their deployment. In practical cybersecurity applications such as real-time DGA botnet detection or anomaly detection in network traffic, barren plateaus can significantly hinder training by preventing effective gradient updates. This leads to slow convergence or failure to learn meaningful decision boundaries, particularly when models must adapt continuously to evolving attack patterns. As a result, optimization challenges directly affect detection latency and model reliability, limiting the feasibility of deploying deep variational circuits in time-sensitive security operations.

8.3 | Limited Real-World Testing

The testing for QML in cybersecurity has largely been based on controlled evaluations. There have been some promising reports, such as the 91.2% detection rate for DGA botnets in [39]. However, the majority of existing works have used static, pre-processed datasets and simulated settings rather than live network environments. They assume ideal conditions, which is not the case in real-world deployments that are infested with noise and adversarial conditions. Models trained on idealistic, curated data may fail when faced with adaptive attacks, evolving malware, or high-volume, dynamic traffic.

8.4 | Explainability & Transparency Gaps

QML systems for cybersecurity are mostly black-boxes. They offer limited interpretability. This becomes problematic in operations where the justification of the labeling of an activity as malicious is demanded. Some approaches, such as Permutation Importance and Accumulated Local Effects, have been explored in the past, but they have been shown to be resource-intensive and inconsistent across implementations. The lack of explainability hinders the adoption of QML due to a lack of analyst trust.

8.5 | Quantum Vs. Classical Crypto Risk

As with any technology, quantum computations can both be used and misused. QML is powerful not in defense, but has powerful capabilities in offence. Large-scale quantum computers endanger classical cryptographic schemes and provide hard-to-counter mechanisms. Marengo and Santamato [25] show that migration toward PQC is urgent for infrastructures that rely on classical encryption. If cryptography is not simultaneously migrated from classical to quantum architectures, it can expose sensitive data to future quantum-based attacks. Thus, QML adoption must be accompanied with broader resilience strategies.

8.6 | High Cost & Access Barriers

To implement QML pipelines at operational scale, teams must manage high costs, limited quantum hardware availability, and complex toolchains. Studies like [27] and [45] show that such demands benefit only well-funded organizations, leaving smaller ones and low-resource regions at a disadvantage, restricting broader participation and creating a divide in cybersecurity.

8.7 | Lack of Regulatory Frameworks

Current cybersecurity regulations are insufficient to support responsible QML deployment, and limit its safe adoption. As noted in [10], challenges persist in areas such as accountability for algorithmic decisions, international data governance, privacy protection, and ethical AI compliance. These shortcomings may result in inconsistent standards and biased protections. Also, early adoption without strong oversight could heighten risks of misuse and uneven security enforcement.

8.8 | Deployment Readiness

Despite promising results, real-world deployment of QML remains limited. Current NISQ hardware suffers from noise, limited qubit counts, and short coherence times, which restrict scalability and reliability. Additionally, access to quantum hardware is costly and often restricted to cloud-based providers, creating economic barriers. These constraints make large-scale, real-time cybersecurity deployment challenging, necessitating hybrid quantum–classical approaches as an intermediate solution. In summary, QML for cybersecurity faces critical challenges including hardware constraints, optimization instability, limited real-world validation, lack of interpretability, high implementation costs, and absence of mature regulatory frameworks. Addressing these issues is essential before QML can transition from experimental research to large-scale deployment [72].

9 | Future Work

As QML for cybersecurity continues to become increasingly explored, the limitations outlined above highlight the need for more operationally grounded research practices that are rigorous and transparent. Addressing these gaps will not only improve scientific reliability but also strengthen real-world applicability across adversarial environments and reproducibility. The following directions outline practical steps that can be taken to build a more robust and secure foundation for future work.

Transparent reporting and leakage-aware benchmarks: There is a need for benchmark suites that capture temporally ordered and streaming data, accurately representing the telemetry and workflow behavior of real SQCs. In QML-based cybersecurity pipelines, such benchmarks are particularly important because temporal leakage can lead to unrealistic advantages when evaluating hybrid quantum–classical classifiers. Additionally, for every experiment, full resource usage must be reported. Resources like the number of queries issued, short budgets, latency, throughput, memory footprint, and total monetary cost

need to be reported. Performance metrics such as accuracy and calibration quality, confidence intervals, and drift statistics over time also have to be studied. By publishing fixed dataset splits and random seeds, reproducibility can be ensured. It can also be ensured by producing auditable checks preventing cross-task or temporal leakage. Thus, limited qubit lifetimes, gaps in the interpretability of models, optimization bottlenecks, and limited hardware remain problems, but the pace of current research indicates progress toward practical and high-fidelity deployment of QML in cybersecurity, constrained operators. Pre-mitigation and on-the-fly shot scheduling can be compared under equal budgets, while longitudinal tracking of calibration drift quantifies accuracy–latency–cost trade-offs across versions. Drift-aware online learning with warm starts and budgeted hyperparameter optimization can be implemented to maintain performance under shift. Specific properties related to the hardware and data, such as gate sets, noise levels, restricted operations, and so forth, can be kept in consideration while choosing encodings and shallow-depth prompting. In QML-driven intrusion detection, these encoding choices may also influence how robust the model is to adversarial manipulation. The drift of calibrations in hardware should be continuously monitored when quantifying accuracy-delay-cost comparisons. To maintain performance under shift, drift-aware online learning with warm starts and budgeted parameter tuning can be implemented. On-the-fly shot scheduling, and doing so before correction, can be compared under equal budgets.

Governance, tooling, and community standards: Structured checklists that record where datasets came from, which prompt or model version was used, and whether any training leaks were prevented can make research cleaner and more trustworthy. In the context of QML for cybersecurity, such governance helps ensure that hybrid quantum pipelines remain auditable and reproducible. When results are reported through a shared result card format and failures are labeled using the same taxonomy, systems can be compared fairly instead of loosely. Public red-team datasets and open scoreboards add transparency by showing how models actually behave under stress tests, rather than only in ideal settings. Finally, community challenges and recognition badges can encourage researchers to fully reproduce and validate entire pipelines instead of stopping at headline numbers, promoting healthy research. In security-sensitive decision systems, blockchain-based decentralized models can provide transparent and tamper-resistant recording of inputs and outcomes, as demonstrated in decentralized credit-scoring applications [73]. Similar provenance mechanisms may improve the auditability of future QML cybersecurity pipelines.

Privacy-preserving analytics and compliance: Trade-offs in privacy and utility can first be measured across real workloads to understand how much functionality is lost when stronger protections are applied. These protections may include differential privacy, trusted execution environments (TEEs), and PQC. In QML-enabled threat detection systems, privacy-preserving computation is particularly relevant because quantum embeddings may expose structure in sensitive telemetry if not properly shielded. Each of these protections should be evaluated for how well they secure data while it is actively being used. Encrypted-traffic analytics and metadata-level telemetry aggregation can then be advanced to operate without inspecting payloads at all. Finally, the compliance impact of these techniques can be documented for domain-specific audits and policy alignment.

Robustness and safety evaluation: Red-team setups can deliberately launch different kinds of attacks such as evasion, data poisoning, and even quantum-aware cross-domain attacks, to proactively break the system and reveal weak points. For QML models used in cybersecurity, such tests can evaluate whether quantum feature maps or variational circuits introduce new attack surfaces. Instead of relying on average performance, evaluation should focus on worst-case behavior, failure modes, and how the system reacts when the attacker adapts. Then, formal multi-stage threat models can be used to design certified defenses and to set training objectives that explicitly target robustness rather than just accuracy [74].

Systems, partitioning, and scheduling: Performance can be improved by intelligently splitting tasks across machines, grouping them together, and reusing stored results, so that the systems remain fast and do not overspend energy and money unnecessarily. When QML components are part of a broader cybersecurity monitoring pipeline, this system-level tuning directly influences TTD and alert reliability. While scheduling the jobs, the scheduler should follow a fixed budget (shots, compute time, etc.) but still hit targets like throughput, worst-case latency, and detection time. Containers can be used to package workflows for automated testing and to ensure that data formats and compiled code stay valid every time we deploy. Reconfigurable hardware such as FPGAs has been investigated for low-latency, high-throughput, and energy-aware processing in next-generation communication infrastructure [75]. In hybrid QML cybersecurity pipelines, such hardware may accelerate classical preprocessing, feature extraction, packet processing, or post-processing while quantum resources are reserved for selected learning operations.

10 | Conclusions

QML gives new hope for cybersecurity by combining quantum computation with machine learning. QML can improve detection accuracy, expose hidden anomalies, adapt to evolving threats in real time, improving much over rule-based and traditional machine learning based systems. In this review, applications of QML across healthcare, malware and botnet detection, and telecommunication security have been surveyed. QSVMs, QNNs, VQCs, and QGANs based frameworks were shown to excel in both supervised and unsupervised settings. Although, hybrid qunatum-classical models, in the current NISQ era, have hardware constraints, strong potential still surfaced across studies. These findings highlight rapid progress of the field towards maturity. Limited qubit lifetimes, gaps in the interpretability of models, optimization bottlenecks, and limited hardware remain problems, but the pace of current research indicates progress toward practical and high-fidelity deployment of QML in cybersecurity. As experimental platforms and learning techniques continue to improve, QML is positioned to support more robust, scalable, and context-aware security systems capable of addressing increasingly complex threat landscapes.

Author Contributions

Siva Sai: conceptualization, literature review, research methodology, and initial manuscript preparation. **Ishika Goyal:** literature review,

data collection, analysis of quantum machine learning techniques, and manuscript editing. **Shubham Sharma:** investigation, taxonomy development, comparative analysis, and visualization of the proposed framework. **Sri Harshita Manuri:** literature synthesis, cybersecurity-related analysis, interpretation of findings, and manuscript review. **Vinay Chamola:** supervision, research methodology, critical evaluation of the proposed taxonomy, and manuscript revision. **Rajkumar Buyya:** research supervision, conceptual guidance, critical review, and final approval of the manuscript.

Acknowledgments

This work was supported by CHANAKYA Fellowship Program of TIH Foundation for IoT & IoE (TIH-IoT) received by Dr. Vinay Chamola under Project Grant File CFP/2022/027 and an ARC Discovery Project.

Funding

This work was supported by the CHANAKYA Fellowship Program of TIH Foundation for IoT & IoE (Grant No. CFP/2022/027).

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

References

1. M. S. Peelam, S. Sai, and V. Chamola, "Explorative Implementation of Quantum Key Distribution Algorithms for Secure Consumer Electronics Networks," *IEEE Transactions on Consumer Electronics* 70, no. 3 (2024): 5576–5584.

2. F. Hossain, K. Hasan, A. Amin, and S. Mahmud, "Quantum Machine Learning for Enhanced Cybersecurity: Proposing a Hypothetical Framework for Next-Generation Security Solutions," 2024.

3. A. Awasthi, "The Role of Quantum Machine Learning in Cybersecurity," *International Research Journal of Modernization in Engineering Technology and Science* 7, no. 1 (2025): 5223–5228.

4. X. Cheng, Y. Chen, X. Yang, H. Zhou, L. Luo, and D. Guo, "Memory-Efficient Programmable Packet Parsing for Multi-Tenant Terabit Networks," *Computer Networks* 264 (2025): 111240.

5. S. Sai and R. Buyya, "Quantum Artificial Intelligence for Mission-Critical Systems: Foundations, Architectural Elements, and Future Directions," *Future Generation Computer Systems* 184 (2026): 108602, https://www.sciencedirect.com/science/article/pii/S0167739X26002360.

6. Data Intelo, "Quantum AI Malware Detection Market Research Report 2024–2032," 2024 accessed online, https://dataintelo.com/report/quantum-ai-malware-detection-market.

7. A. Sundaram, "Challenges and Opportunities in Quantum Computing in Healthcare," in *Quantum Computing for Healthcare Data*, ed. G. Nagasubramanian, S. Rakesh Kumar, and E. B. Valentina (Academic Press, 2025), 91–118, https://doi.org/10.1016/B978-0-443-29297-2.00010-1.

8. K. Gupta, D. Saxena, P. Rani, et al., "An Intelligent Quantum Cyber-Security Framework for Healthcare Data Management," *IEEE Transactions on Automation Science and Engineering* 22 (2024): 6884–6895.

9. H. Suryotrisongko and Y. Musashi, "Evaluating Hybrid Quantum-Classical Deep Learning for Cybersecurity Botnet DGA Detection," in *Procedia Computer Science*, vol. 197 (2022), 223–229.

10. S. Nokhwal, S. Nokhwal, S. Pahune, and A. Chaudhary, "Quantum Generative Adversarial Networks: Bridging Classical and Quantum Realms," in *Proceedings of the 2024 8th International Conference on Intelligent Systems, Metaheuristics & Swarm Intelligence* (2024), 105–109.

11. S. Raj, S. Sai, Y. Simmhan, K. Chard, and R. Buyya, "Quantum Integrated High-Performance Computing: Foundations, Architectural Elements and Future Directions," 2026 arXiv:2604.19814.

12. T. Nguyen, T. Sipola, and J. Hautamäki, "Machine Learning Applications of Quantum Computing: A Review," 2024.

13. V. Ganapathy, "Quantum Machine Learning for Anomaly Detection in Cyber Security Audits," *Shodh Sari—An International Multidisciplinary Journal* 4, no. 1 (2025): 127–154.

14. S. K. Dornala and P. Senthilkumar, "A Comprehensive Survey on Intelligent Firewall-Based Malware Detection Using Proactive and Quantum Approaches," *International Journal of Computer Networks and Wireless Communications (IJCNWC)* 15, no. 2 (2025): 1123–1133.

15. L. Eze, U. B. Chaudhry, and H. Jahankhani, "Quantum-Enhanced Machine Learning for Cybersecurity: Evaluating Malicious URL Detection," *Electronics* 14, no. 9 (2025): 1827.

16. M. S. Peelam, A. A. Rout, and V. Chamola, "Quantum Computing Applications for Internet of Things," *IET Quantum Communication* 5, no. 2 (2024): 103–112.

17. D. Wierichs, J. Izaac, C. Wang, and C. Y.-Y. Lin, "General Parameter-Shift Rules for Quantum Gradients," *Quantum* 6 (2022): 677.

18. W. Sun, Y. Jin, G. Lu, and Y. Liu, "Stabilizer Testing and Central Limit Theorem," *Physical Review A* 111, no. 3 (2025): 032421.

19. S. Lloyd, M. Mohseni, and P. Rebentrost, "Quantum Algorithms for Supervised and Unsupervised Machine Learning," 2013 arXiv:1307.0411.

20. S. Shao, Y. Tian, Y. Zhang, and X. Zhang, "Knowledge Learning-Based Dimensionality Reduction for Solving Large-Scale Sparse Multiobjective Optimization Problems," *IEEE Transactions on Cybernetics* 55, no. 7 (2025): 3471–3484.

21. F. Ding, Z. Liu, Y. Wang, et al., "Intelligent Event Triggered Lane Keeping Security Control for Autonomous Vehicle Under dos Attacks," *IEEE Transactions on Fuzzy Systems* 33, no. 10 (2025): 3595–3608.

22. T. Alladi, V. Kohli, V. Chamola, and F. R. Yu, "Securing the Internet of Vehicles: A Deep Learning-Based Classification Framework," *IEEE Networking Letters* 3, no. 2 (2021): 94–97.

23. G. K. Verma, B. Singh, N. Kumar, and V. Chamola, "CB-CAS: Certificate-Based Efficient Signature Scheme With Compact Aggregation for Industrial Internet of Things Environment," *IEEE Internet of Things Journal* 7, no. 4 (2019): 2563–2572.

24. V. Chamola, A. Jolfaei, V. Chanana, P. Parashari, and V. Hassija, "Information Security in the Post Quantum Era for 5g and Beyond Networks: Threats to Existing Cryptography, and Post-Quantum Cryptography," *Computer Communications* 176 (2021): 99–118.

25. A. Marengo and V. Santamato, "Quantum Algorithms and Complexity in Healthcare Applications: A Systematic Review With Machine Learning-Optimized Analysis," *Frontiers in Computer Science* 7 (2025): 1584114.

26. S. Lloyd and C. Weedbrook, "Quantum Generative Adversarial Learning," *Physical Review Letters* 121, no. 4 (2018): 040502.

27. M. G. Tehrani, "Quantum Cybersecurity Analytics: Evaluation of Hybrid QML for DGA Botnet Detection," 2024 PhD dissertation, The George Washington University.

28. O. A. Oyebode and A. A. Jimoh, "Quantum Cryptography in Telecommunication Systems: Securing Data Transmission Against Emerging Cyber Threats," *International Journal of Computer Applications Technology and Research* 14 (2025): 147–162.

29. K. Zhang, H. Wang, M. Chen, et al., "Leveraging Machine Learning to Proactively Identify Phishing Campaigns Before They Strike," *Journal of Big Data* 12, no. 1 (2025): 124.

30. G. Karamchand, "Quantum Machine Learning for Threat Detection in High-Security Networks," *Samriddhi: A Journal of Physical Sciences, Engineering and Technology* 17, no. 2 (2025): 14–25.

31. A. K. Sharma, M. S. Peelam, B. K. Chauasia, and V. Chamola, "Qiotchain: Quantum IoT-Blockchain Fusion for Advanced Data Protection in Industry 4.0," *IET Blockchain* 4, no. 3 (2024): 252–262.

32. Y. Zhou, T. Luo, Z. He, G. Jiang, H. Xu, and C.-C. Chang, "Caisformer: Channel-Wise Attention Transformer for Image Steganography," *Neurocomputing* 603 (2024): 128295.

33. T. Luo, R. Hu, Z. He, et al., "DiffW: Multi-Encoder Based on Conditional Diffusion Model for Robust Image Watermarking," *IEEE Transactions on Multimedia* 28 (2025): 837–852.

34. S. Sai, V. Hassija, V. Chamola, and M. Guizani, "Federated Learning and NFT-Based Privacy-Preserving Medical-Data-Sharing Scheme for Intelligent Diagnosis in Smart Healthcare," *IEEE Internet of Things Journal* 11, no. 4 (2023): 5568–5577.

35. S. Sai, V. Chamola, K.-K. R. Choo, B. Sikdar, and J. J. Rodrigues, "Confluence of Blockchain and Artificial Intelligence Technologies for Secure and Scalable Healthcare Solutions: A Review," *IEEE Internet of Things Journal* 10, no. 7 (2022): 5873–5897.

36. J. Jin, M. Wu, A. Ouyang, K. Li, and C. Chen, "A Novel Dynamic Hill Cipher and Its Applications on Medical IoT," *IEEE Internet of Things Journal* 12, no. 10 (2025): 14297–14308.

37. D. Li, S. Ren, H. Wang, J. Liu, and S. S. Ge, "Randomized Average Consensus Based on Additive Privacy Sharing," *Automatica* 186 (2026): 112847.

38. M. Al-Hawawreh and M. S. Hossain, "A Human-Centered Quantum Machine Learning Framework for Attack Detection in IoT-Based Healthcare Industry 5.0," *IEEE Internet of Things Journal* 12, no. 22 (2025): 46065–46074.

39. M. Tehrani, E. Sultanow, W. J. Buchanan, et al., "Enabling Quantum Cybersecurity Analytics in Botnet Detection: Stable Architecture and Speed-Up Through Tree Algorithms," 2023 arXiv:2306.13727.

40. D. Abreu, C. E. Rothenberg, and A. Abelém, "QML-IDS: Quantum Machine Learning Intrusion Detection System," in *2024 IEEE Symposium on Computers and Communications (ISCC)* (IEEE, 2024), 1–6.

41. K. Zhang, Y. Wang, U. A. Bhatti, Y. Zhou, and M. Jin, "Enhanced Ransomware Attacks Detection Using Feature Selection, Sensitivity Analysis, and Optimized Hybrid Model," *Journal of Big Data* 12, no. 1 (2025): 245.

42. T. Bikku, S. B. Chandolu, S. P. Praveen, N. R. Tirumalasetti, K. Swathi, and U. Sirisha, "Enhancing Real-Time Malware Analysis With Quantum Neural Networks," *Journal of Intelligent Systems & Internet of Things* 12, no. 1 (2024): 57–69.

43. G. Barrué and T. Quertier, "Quantum Machine Learning for Malware Classification," in *Joint European Conference on Machine Learning and Knowledge Discovery in Databases* (Springer Nature Switzerland, 2023), 245–260.

44. E. Krátká and A. G. Gábris, "Quantum Computing Methods for Malware Detection," in *Machine Learning, Deep Learning and AI for Cybersecurity* (Springer Nature Switzerland, 2025), 207–228.

45. P. Noah and D. Alexander, "Quantum Machine Learning for Enhancing Cybersecurity in 5g Networks," 2023.

46. D. K. Kejriwal, A. Goel, and A. Sharma, "Advancing Adversarial Robustness in Cybersecurity: Gradient-Free Attacks and Quantum-Inspired Defenses for Machine Learning Models," *International Journal of Innovative Science and Research Technology* 10, no. 4 (2025): 54–65.

47. Y. A. Ergu, V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, "Q-Poison: Quantum Adversarial Attacks Against QML-Driven Interference Classification in o-Ran," in *2025 IEEE International Conference on Machine Learning for Communication and Networking (ICMLCN)* (Elsevier, 2025), 1–6.

48. J. Huang, M. Wen, M. Wei, and Y. Bi, "Enhancing the Transferability of Adversarial Samples With Random Noise Techniques," *Computers & Security* 136 (2024): 103541.

49. G. Bologna and Y. Hayashi, "QSVM: A Support Vector Machine for Rule Extraction," in *International Work-Conference on Artificial Neural Networks* (Springer International Publishing, 2015), 276–289.

50. U. R. Janak, *Detection of Cyber Attacks on Power Distribution System Using QSVM*," M.Sc. thesis (Purdue University, 2024), 12.

51. M. Y. Küçükkara, F. Atban, and C. Bayilmiş, "Quantum-Neural Network Model for Platform-Independent DDOS Attack Classification in Cyber Security," *Advanced Quantum Technologies* 7, no. 10 (2024): 2400084.

52. M. A. Rahman, M. S. Akter, E. Miller, et al., "Fine-Tuned Variational Quantum Classifiers for Cyber Attacks Detection Based on Parameterized Quantum Circuits and Optimizers," in *2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)* (Elsevier, 2024), 1067–1072.

53. P. You, P. Chen, X. Li, and A. Bian, "Gated Memory-Guided Multi-Scale Spatio–Temporal–Spectral Feature Fusion Network for Unsupervised Internet of Things Time Series Anomaly Detection," *Engineering Applications of Artificial Intelligence* 169 (2026): 114104.

54. W. E. Maouaki, N. Innan, A. Marchisio, T. Said, M. Bennai, and M. Shafique, "Quantum Clustering for Cybersecurity," in *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)*, vol. 2 (Elsevier, 2024), 5–10.

55. J. Chen, X. Qi, L. Chen, F. Chen, and G. Cheng, "Quantum-Inspired Ant Lion Optimized Hybrid k-Means for Cluster Analysis and Intrusion Detection," *Knowledge-Based Systems* 203 (2020): 106167.

56. M. A. Rahman, H. Shahriar, V. Clincy, M. F. Hossain, and M. Rahman, "A Quantum Generative Adversarial Network-Based Intrusion Detection System," in *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)* (2023), 1810–1815.

57. F. Cirillo and C. Esposito, "Intrusion Detection System Based on Quantum Generative Adversarial Network," in *Proceedings of the 17th International Conference on Agents and Artificial Intelligence (ICAART 2025)* (SCITEPRESS–Science and Technology Publications, LDA, 2025), 830–838.

58. S. Sai, I. Goyal, V. Chamola, and R. Buyya, "Generative Ai in the Age of Quantum Computing: A Taxonomy, Architectural Elements and Future Directions," *Future Generation Computer Systems* 185 (2026): 108714, https://www.sciencedirect.com/science/article/pii/S0167739X26003481.

59. C. Li, D. Hu, G. Liu, Y. Wen, J. Wei, and Z. Tang, "MC-ORAM: A Concurrent ORAM Scheme for Multi-User Shared Storage," *IEEE Transactions on Computers* 75, no. 7 (2026): 2406–2420.

60. L. Zeng, Y. Chang, X. Zhang, et al., "Distributed Machine Learning Based on Quantum Cloud With Quantum Homomorphic Encryption," *Future Generation Computer Systems* 175 (2026): 108053.

61. Y. Liu, B. Zhao, M. Zhai, et al., "Multi-Leader Byzantine Fault Tolerance in Blockchain: Performance and Security," *IEEE Transactions on Information Forensics and Security* 21 (2026): 1622–1637.

62. Y. Wang, X. He, Z. Cai, et al., "Fedcompass: Federated Clustered and Periodic Aggregation Framework for Hybrid Classical-Quantum Models," 2026 arXiv:2602.03052.

63. R. Zhang, Y. Wang, X. He, et al., "QFI-OPT: Communication-Efficient Quantum Federated Learning via Quantum Fisher Information," *Software: Practice and Experience* 56, no. 3 (2026): 289–316.

64. D. B. Salvakkam, V. Saravanan, P. K. Jain, and R. Pamula, "Enhanced Quantum-Secure Ensemble Intrusion Detection Techniques for Cloud Based on Deep Learning," *Cognitive Computation* 15, no. 5 (2023): 1593–1612.

65. R. Gupta, D. Saxena, I. Gupta, A. Makkar, and A. K. Singh, "Quantum Machine Learning Driven Malicious User Prediction for Cloud Network Communications," *IEEE Networking Letters* 4, no. 4 (2022): 174–178.

66. P. Kaliyamoorthy and A. C. Ramalingam, "Qmlfd Based Rsa Cryptosystem for Enhancing Data Security in Public Cloud Storage System," *Wireless Personal Communications* 122 (2022): 755–782.

67. R. Maddali, "Ai-Driven Quality Assurance in Cloud-Based Data Systems: Quantum Machine Learning for Accelerating Data Quality Metrics Calculation," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 8, no. 4 (2022): 366–382.

68. S. Sai, A. Sawaika, P. Singh, and R. Buyya, "Quantum Federated Learning: Architectural Elements and Future Directions," in *Federated Learning: Foundations and Applications* (Morgan Kaufmann, 2026), 325–343.

69. L. Lin, R. Ma, Z. Wang, et al., "HWDSQP: A Historical Weighted and Dynamic Scheduling Quantum Protocol to Enhance Communication Reliability," *IEEE Journal on Selected Areas in Communications* 43 (2025): 2810–2824.

70. B. Khanal, P. Rivas, A. Sanjel, K. Sooksatra, E. Quevedo, and A. Rodriguez, "Generalization Error Bound for Quantum Machine Learning in the NISQ Eraa Survey," *Quantum Machine Intelligence* 6, no. 2 (2024): 90.

71. J. Cunningham and J. Zhuang, "Investigating and Mitigating Barren Plateaus in Variational Quantum Circuits: A Survey," *Quantum Information Processing* 24, no. 2 (2025): 48.

72. Y. Zhang, S. Feng, P. Wang, et al., "Learning Self-Growth Maps for Fast and Accurate Imbalanced Streaming Data Clustering," *IEEE Transactions on Neural Networks and Learning Systems* 36, no. 9 (2025): 16049–16061.

73. V. Hassija, G. Bansal, V. Chamola, N. Kumar, and M. Guizani, "Secure Lending: Blockchain and Prospect Theory-Based Decentralized Credit Scoring Model," *IEEE Transactions on Network Science and Engineering* 7, no. 4 (2020): 2566–2575.

74. W. Zhang, W. Fan, W. Su, and N. Bouguila, "HKANLP: Link Prediction With Hyperspherical Embeddings and Kolmogorovarnold Networks," *IEEE Transactions on Neural Networks and Learning Systems* 37, no. 2 (2026): 966–980.

75. V. Chamola, S. Patra, N. Kumar, and M. Guizani, "FPGA for 5g: Re-Configurable Hardware for Next Generation Communication," *IEEE Wireless Communications* 27, no. 3 (2020): 140–147.