Received: 31 December 2024 | Revised: 10 April 2025 | Accepted: 7 May 2025 | Published online: 3 September 2025

RESEARCH ARTICLE

Journal of Computational and Cognitive Engineering
2026, Vol. 5(1) 16–29
DOI: 10.47852/bonviewJCCE52025121

BON VIEW PUBLISHING

A Hybrid Framework Integrating QML, AI, and Quantum-Safe Cryptography for Cybersecurity

Ramasubramaniyan Gunasridharan[1], Ali Altalbe[2], Bharathi Mohan Gurusamy[3], Gundala Pallavi[3] and Prasanna Kumar Rangarajan[3,*]

[1] *Department of Computer Engineering, Birla Institute of Technology and Science, India*

[2] *Faculty of Computing and Information Technology, King Abdulaziz University, Saudi Arabia*

[3] *Department of Computer Science and Engineering, Amrita Vishwa Vidyapeetham-Chennai, India*

Abstract: The rise of quantum computing poses threats to traditional cryptographic systems, thereby requiring security measures to safeguard against traditional and quantum-attacker cyber insecurity. This framework uses quantum machine learning (QML) algorithms along with quantum-safe encryption to boost security measures. The proposed system combines QML anomaly detection models variational quantum classifier (VQC) with quantum support vector classifier (QSVC) as well as quantum neural network and examines them based on the BB84 QKD protocol for information safety. This model was evaluated using three datasets of HIKARI Flow intrusion detection records, phishing activity logs, and malicious URLs. This includes all high-dimensional input by extensive application of feature engineering, which merges entropy scoring combined with keyword extraction and domain analysis to transmogrify it into suitable inputs for quantum processing. The QML models outperformed the traditional models with a maximum phishing detection accuracy of 97.75% by QSVC implementation. With the BB84 protocol, its eavesdropping detection was proved by quantum interference detection upon testing on IBM's Qiskit and Google's Cirq systems while the operations were secure and in attack scenarios. This system combines the latest features to address the limitations of the current AI security model and incorporates post-quantum cryptography to protect against quantum threats. In conclusion, QML and quantum cryptography work efficiently with operational cybersecurity platforms.

Keywords: quantum cryptography, threat detection, quantum key distribution, post-quantum cryptography, hybrid AI-QML security

1. Introduction

In today's digitally connected world, cybersecurity needs to focus on protecting systems, network, data from unauthorized access, disruption, and cyberattacks. Traditional security systems cannot provide protection from these technologically advanced attacks as they rely on predefined and established rules. Security systems have evolved with machine learning (ML) and artificial intelligence (AI) techniques [1], which has successfully enabled cybersecurity assignments including intrusion detection and phishing classification. However, these systems become vulnerable to attacks through AI cybersecurity because attackers deploy the same technological methods to execute data poisoning and evasion attacks [2].

Quantum computing technology causes an instant threat to traditional cryptographic systems that are currently in use. RSA along with elliptic curve cryptography (ECC) depends on the mathematical difficulty of breaking large number factorization for encryption security. Shor's algorithm as a quantum factorization method proves efficient at breaking encryption schemes that makes much of present-day cybersecurity infrastructure susceptible to attack [3]. The development of quantum-safe cryptographic methods including quantum key distribution (QKD) and post-quantum encryption algorithms represents researchers' response to ensure data security in the long term [4].

Even with these developments, AI-powered cybersecurity and quantum cryptography are usually built independently. AI/ML models are mainly used to detect and counter classical cyberattacks, whereas quantum cryptographic methods are meant to be quantum adversary-resistant without using AI-powered anomaly detection [5]. This lack of integration is a key challenge, exposing digital security systems to both adversarial AI attacks and quantum-enabled cryptanalysis.

This research proposes a hybrid cybersecurity approach that uses AI-based anomaly detection and quantum-resilient cryptographic protocols.

The following are the main contributions of this research:

1) A novel hybrid quantum-resistant cryptographic system featuring AI
2) Significant cybersecurity operations involving diverse datasets like intrusion detection along with phishing classification and malicious URL identification
3) A proposed system that solves operating difficulties presented by noisy intermediate-scale quantum (NISQ) devices
4) A comparison study that validates the quantum machine learning (QML)-based security system against standard AI/ML model performances.

The paper is structured as follows: Section 2 provides a detailed literature review of AI-based cybersecurity, quantum computing threats,

*Corresponding author: Prasanna Kumar Rangarajan, Department of Computer Science and Engineering, Amrita Vishwa Vidyapeetham-Chennai, India. Email: r_prasannakumar@ch.amrita.edu

quantum-safe cryptographic methods, and current research gaps. Section 3 summarizes the methodology, explaining data collection, preprocessing, QKD integration, and QML model development. Section 4 discusses the results and a comparison of classical and quantum models of cybersecurity. Last, Section 5 concludes the research and considers possible avenues for future research.

2. Literature Review

The convergence of AI, ML, and quantum-safe cryptography has emerged as a critical part in cybersecurity, stabilizing threats from classical and quantum computing developments. New studies report challenges and opportunities involved in integrating these technologies to support digital security protocols. This section runs toward significant work in this new field. The advent of quantum computers threatens traditionally used cryptographic systems, RSA and ECC, both of which depend on the hardness of factoring large primes. Shor's algorithm, which is a quantum algorithm solving this problem efficiently, would make conventional encryption techniques obsolete [6]. Bernstein [7] presented a thorough examination of why traditional cryptographic protocols are liable to quantum attacks.

Identifying these risks, the National Institute of Standards and Technology (NIST) has initiated efforts to develop post-quantum cryptography (PQC) standards targeted at resisting quantum adversaries. While these cryptographic solutions offer theoretical resistance to quantum attacks, Radanliev [8] critiques their computational overhead and deployment challenges. It recommends using hybrid security systems that link quantum protocol BB84 with AI security models. The combined approach provides a balanced solution according to their argument by integrating scalability capabilities with strengthened resilience against modern and future cyber threats.

2.1. Artificial intelligence and machine learning in cybersecurity

The application of AI and ML has transformed how organizations discover, prevent, and react to cyberattacks. These are superior in pattern detection, anomaly discovery, and automated response to threats and thus must be used in contemporary security systems. Kaur et al. [9] proved the superiority of adversarial ML models in both mimicking cyberattacks and resisting changing attacks, solidifying their implementation in proactive defense systems. Rafy et al. [10] presented deep learning-based intrusion detection models, which achieved the best-in-class accuracy in huge networks by effectively detecting malicious traffic. Likewise, Sehgal and Gupta [11] investigated ML classifiers for URL and phishing and tested their efficacy for real-time email and URL threat detection. Aside from network security, Rios Insua [12] also studied AI-based biometric authentication systems, such as keystroke dynamics, and their potential to improve user authentication against advanced attacks.

However, there are still challenges for AI-based cybersecurity. Avro et al. [13] and Okeke and Omojola [14] pointed out scalability, bias, and deployment limitations, citing that most organizations still rely on unsupervised anomaly detection approaches, which can lead to the research-led innovation–practice gap. In addition, Thakur et al. [15] pointed out the dual-edged nature of ML in cybersecurity, emphasizing its use in both cyber defense and offensive campaigns, including malware detection and spear-phishing attacks. The growing deployment of AI/ML in cybersecurity paradigms also raises ethical and technical concerns. Nag et al. [16] have highlighted the importance of bias mitigation enhancements and scaling to ensure AI-driven security controls are fair, transparent, and effective in deployment environments.

2.2. QML in cybersecurity

QML is an emerging field in cybersecurity, leveraging the capabilities of quantum computing to support threat detection. By combining quantum algorithms with advanced ML models, QML enables more efficient detection and prevention of cyberattacks [17, 18]. Akter et al. [19] showed how a quantum support vector machine (QSVM) detects malware by processing Drebin215 dataset on Pennylane framework. The model achieved 95% accuracy in its operations, which proved the suitability of QML for real-world cybersecurity applications. Rosa-Remedios and Caballero-Gil [20] examined QML models for their ability to forecast cyberattacks by analyzing various cybersecurity databases where QML effectively finds concealed attack signatures as cybersecurity databases gain more significance for future investigations.

QML has also demonstrated tremendous potential in intrusion detection systems (IDS). Abreu et al. [21] designed QML-IDS, a hybrid quantum and classical IDS model, showing a higher classification performance for both binary and multiclass intrusion detection. Ciliberto et al. [22] defined fundamental QML algorithms, such as variational quantum classifiers (VQC) and QSVM, for security use. Later studies focused on certain QML methods for security applications. Rahman et al. [23] employed VQC and quantum feature maps to identify cyber threats in big data, whereas Ciaramella et al. [24] used quantum kernels to improve the accuracy of phishing and malware detection. Kalinin and Krundyshev [25] illustrated the generalization capability of quantum neural networks (QNNs) for complex intrusion patterns that make QNNs a valuable tool for managing dynamic cybersecurity threats.

2.3. Quantum cryptography: BB84 and beyond

QKD provides a cryptographic security solution that allows secure encryption key exchange over insecure communication channels. In 1984, Bennett and Brassard introduced BB84, the most popular QKD protocol today, whose security rests on the principles of fundamental quantum mechanics. The BB84 protocol employs polarized photons together with the uncertainty principle to reveal eavesdropping attempts because any interception produces detectable disturbances in the quantum channel. Multiple experimental investigations have proven that BB84 stands firm against multiple forms of eavesdropping attacks. This shows the protocol stands up to quantum attacks by using IBM Qiskit simulations to validate its performance [26].

The implementation of BB84 in real-world scenarios has significant obstacles because of quantum channel noise and hardware constraints. Research investigations have established new security-improving operational enhancements for BB84 systems. On their thorough analysis of the QKD systems, Reddy et al. [27] explained decoy state protocols and improved error correction methods that defend against complex security threats. The BB84 protocol remains vital for creating enhanced modifications to establish secure communication systems to be adopted in practical applications.

Educational institutions now receive increased access to quantum cryptography technology through recent developments. Bloom et al. [28] created an undergraduate-level experimental setup combining optical components with computational simulations that implemented BB84 to provide students with practical exposure of QKD principles.

Bennett and Brassard [29] extended its scope to include different uses of quantum cryptography beyond key exchange methods. They proved that QKD works together with classical channels to enable secure key establishment without requiring prior shared information. This previous study presented quantum coin-tossing protocols while establishing fundamental principles about quantum mechanics for cryptographic security and exploring the Einstein-Podolsky-Rosen paradox.

2.4. Hybrid frameworks: AI and quantum-safe cryptography

The integration of AI with quantum-resistant cryptography provides a feasible approach to enhancing cybersecurity through adaptive learning processes and quantum-resistant encryption [30]. Majid et al. [31] presented a hybrid model that integrates PQC and ML models, optimizing encryption protocols to enhance the security of data. Their article brings to the fore the need for adaptive cryptographic techniques that can counter quantum-enabled cyberattacks.

Li et al. [32] brought in gradient-free optimizers, including Constrained Optimization By Linear Approximations (COBYLA), for training QML models in NISQ systems. This helps save computational overhead and makes it more efficient, enhancing the practicality of secure quantum architectures. Building on this idea, Dash and Ullah [33] proposed a privacy-preserving federated learning framework, combining fully homomorphic encryption (FHE) with quantum kernels to facilitate secure decentralized data processing. To enhance quantum-resistant cyber resilience, recent advances in cybersecurity have explored hybrid solutions that blend AI, cryptographic techniques, and blockchain-based security architectures.

Unlike isolated cryptographic systems, hybrid AI-QML cybersecurity models employ blockchain for safe data provenance tracking, PQC methods for safe encryption, and ML for anomaly detection. Wang et al. [34] demonstrated how graph convolutional networks and blockchain-based anomaly detection enhance security in smart healthcare environments. Similarly, for secure IoT-based communication, a quantum-safe software-defined IoT approach [35] proposes hardware-backed cybersecurity combining AI and PQC algorithms. Such frameworks exhibit the potential of hybrid models for quantum-resistant cybersecurity integrating decentralized trust mechanisms, cryptography, and AI. Hybrid cryptographic methods have also been examined for enterprise communication security. Rencis et al. [36] proposed a QKD-based hybrid security model that blends the use of classical cryptographic algorithms with quantum-resistant PQC approaches. Their method sets up secure channels of communication by employing QKD links for user authentication and key exchange with smart cards, providing an economical and scalable security paradigm. Building further on these concepts, Fedorov [37] examined hybrid quantum-secured environments, proving the synergy of QKD and PQC for the protection of distributed applications like blockchains.

2.5. Research gaps and challenges

Despite the progress in AI, ML, QML [38], and PCQ, current cybersecurity frameworks do not have an integrated solution that accurately counteracts the classical and quantum cyber threats. Current research is more confined to the AI/ML-based security models or quantum-safe cryptographic methods but hardly considers their collective efficacy in a hybrid AI-QML cybersecurity framework. Table 1 consolidates recent AI-QML cybersecurity research contributions, showcasing their methodologies, strengths, weaknesses, and areas of research gaps. The comparison highlights the need for a hybrid AI-QML framework combining AI-based cyber defense with quantum-resistant cryptographic techniques to deliver greater security against both classical and quantum cyber threats.

The deployment of QML-based cybersecurity systems has multiple essential research obstacles, which are listed in Table 1.

1) NISQ hardware operates with unstable performance and numerous errors that slow down the growth of QML-based cybersecurity solutions.
2) QKD deployment in AI-based cybersecurity systems remains inconsistent because no established protocols exist for its full implementation across different architectures.
3) The implementation of hybrid AI-QML security systems faces difficulties with real-time and large-scale deployment because they need significant computational resources.
4) Secure AI models utilizing QML for cybersecurity protection can develop into security risks when adversaries misuse them through automated methods for security evasion attacks.

Mitigating such challenges requires more research into:

1) The development of uniform security guidelines needs to focus exclusively on protecting AI-QML cybersecurity systems.
2) The development of ethical frameworks along with regulatory rules must occur to stop malicious QML technology uses.
3) This research helps reduce existing gaps through its proposed combination of AI and QML cybersecurity systems.

The present study aims to bridge existing gaps by implementation of an AI-QML cybersecurity framework that combines multiple components. The integration of QML-based threat detection models with quantum-resistant encryption schemes enhances cybersecurity resistance to cyberattacks.

Table 1
Comparison of recent AI-QML cybersecurity studies

Reference	Method	Strength	Limitations	Research Gap
[39]	Theoretical framework for enhancing threat detection and encryption	Highlights QML potential in security	Limited experimental validation and lacks real-world implementation	Standardizing quantum integration and practical deployment
[40]	Hybrid quantum security for botnet detection	Quantum speed-up and accuracy improvements	High execution time and hardware dependent	Optimization for practical QML cybersecurity analytics
[41]	Red teaming approach to analyze cybersecurity risks	Assesses quantum security measures	Theoretical focus lacks practical deployment	Needs real-world application
[42]	PCA-based intrusion detection using QML	Achieving quantum advantage in cybersecurity	Scalability concerns, high computational requirements	Exploration in QML's application of broader cybersecurity tasks
[43]	Quantum-enhanced Zero Trust Framework (QNN-ZTF) for anomaly detection	Strengthens Zero Trust security; Introduces adaptive quantum anomaly detection	Scalability concerns; high computational requirements	Optimization is needed

3. Methodology

The AI-QML cybersecurity model provides a systematic approach, which integrates data-driven threat intelligence, quantum cryptographic security, and quantum-enhanced ML algorithms. This process has five main phases:

1) Data collection and preprocessing
2) Quantum cryptography implementation
3) Development of QML models
4) Optimization methods
5) Security validation and deployment

Figure 1 presents the entire research workflow that follows a systematic methodology starting from data retrieval and processing through quantum-enhanced secure threat identification.

3.1. Dataset collection and preprocessing

This research examines QML model performances through assessment of HIKARI Flow, Phishing, and Malicious URL datasets, which are widely recognized in cybersecurity fields. The selected datasets support security operations by detecting intrusions and classifying phishing attacks and web links, which establishes their usefulness in analyzing QML efficiency under practical threat conditions.

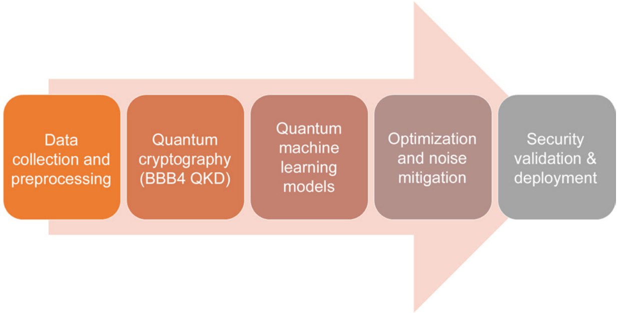
3.1.1. Preprocessing and feature engineering

To achieve compatibility with QML models, the gathered datasets are cleaned, normalized, and transformed into features. Feature engineering is conducted to extract the prominent attributes that facilitate intrusion detection, phishing classification, and malicious URL detection.

The HIKARI Flow dataset depends on entropy scores to evaluate network packet randomness for detecting anomalies. The analysis examined flow duration as an additional feature, which joins protocol type and port usage features to detect suspicious behaviors that might indicate attack patterns. The Phishing dataset was used to detect phishing content by analyzing two indicator types, which include urgent or password keywords and email header inconsistencies and URL length and domain age measurements. The malicious URL dataset was evaluated using URL entropy assessments together with subdomain complexity metrics and domain registration period measurements to detect malicious behavior.

The standardization technique underlines all numerical dataset features as it transforms them into a [0,1] value range. The analysis of complex cybersecurity datasets achieves higher effectiveness with VQC and quantum support vector classifier (QSVC) and QNN QML models because of their implementation of statistical features that derive entropy measurements and anomalous scoring and interaction terms.

Figure 1
AI-QML cybersecurity methodology workflow


Data collection and preprocessing
Quantum cryptography (BBB4 QKD)
Quantum machine learning models
Optimization and noise mitigation
Security validation & deployment

The BB84 QKD protocol provides secure key exchange for the process before detecting protected communication. The QML models operate using improved data inputs, which both boost their learning algorithms and enhances protection of the system against classical and quantum cyber threats.

3.2. Quantum cryptography implementation

We tested the protocol through simulations executed with IBM Qiskit and Google Cirq platforms, which created environments for testing BB84 using secure conditions and situations where attackers tried to detect its communication.

The protocol underwent two test scenarios where successful key exchange protected secure communication between the sender and the receiver occurred first and then an eavesdropper's attempted interception generated detectable disturbances. The simulated cryptographic keys became part of the extended QML threat detection system, which strengthened security against quantum and classical source attacks.

3.2.1. Theoretical design

The BB84 protocol involves the following steps, as summarized in Algorithm 1:

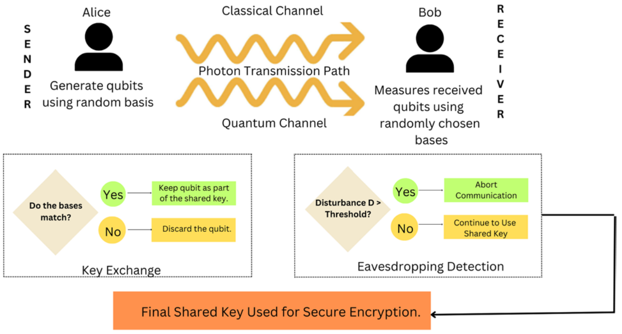
Algorithm 1: BB84 Quantum key distribution

```
1. Alice prepares qubits: $|\psi\rangle = \{ |0\rangle, |1\rangle, |+\rangle, |-\rangle \}$, encoded in random bases $\{+, \times\}$.
2. Alice sends qubits → Bob via the quantum channel.
3. Bob measures each qubit in a randomly chosen basis $\{+, \times\}$.
4. Alice and Bob announce bases over a classical channel.
5. Key Agreement:
   If basis(Alice) = basis(Bob), keep qubit in key.
   Otherwise, discard qubit.
6. Eavesdropping Check:
   Compute error rate: $D = |M\_A \oplus M\_B| / N$.
   If $D >$ threshold, abort communication.
7. Final secure key: K = {retained qubits}.
    $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ → Qubit states
    $+, \times$ → Rectilinear and diagonal bases
    M_A, M_B → Alice's and Bob's measured qubits
    N → Number of compared qubits
    K → Final shared key
```

The BB84 QKD protocol guarantees the secure exchange of keys through the use of quantum superposition and measurement disturbance for the detection of eavesdropping. The sender (Alice) first generates qubits, randomly encoding them in either the rectilinear (+, −) or diagonal (×, ÷) basis. They were sent over a quantum channel to the receiver (Bob), who measures every qubit with a randomly chosen basis. After the quantum transmission, Alice and Bob exchange over a classical channel to identify the basis they used. Only qubits measured in the same basis are kept to create the final cryptographic key, whereas others are discarded. Any difference above a threshold shows that there exists an eavesdropper (Eve), thus providing security before key use.

Figure 2 describes the BB84 QKD protocol, depicting interaction between Alice (sender) and Bob (receiver) via both quantum and classical

Figure 2
Flow diagram of the BB84 quantum key distribution protocol


SENDER
Alice
Generate qubits using random basis
Classical Channel
Photon Transmission Path
Quantum Channel
Bob
Measures received qubits using randomly chosen bases
RECEIVER
Do the bases match?
Yes
Keep qubit as part of the shared key.
No
Discard the qubit.
Key Exchange
Disturbance D > Threshold?
Yes
Abort Communication
No
Continue to Use Shared Key
Eavesdropping Detection
Final Shared Key Used for Secure Encryption.

channels. The figure indicates key exchange steps, eavesdropping detection, and ultimate encryption. To simulate the BB84 protocol, a quantum circuit model is constructed utilizing quantum computing paradigms. Figure 3 illustrates the quantum circuit employed in BB84 implementation, in which qubits (q_0, q_1, …, q_n) are used for encoding and transmission as the quantum bits. Hadamard gates (H) are used to achieve superposition so that qubits can be in more than one state at the same time. Measurement gates decide the ultimate qubit states upon transmission.

The circuit mimics Alice encoding a random string of qubits and sending them over a quantum channel and Bob measuring them with randomly chosen bases. When Eve tries to intercept the qubits, the no-cloning theorem and quantum measurement rules induce inconsistencies in Bob's received string, introducing measurable perturbations in the quantum channel. These interruptions enable Alice and Bob to identify tampering and guarantee that only a secure key is utilized for cryptographic processes (Figure 3).

3.2.2. Simulation environment

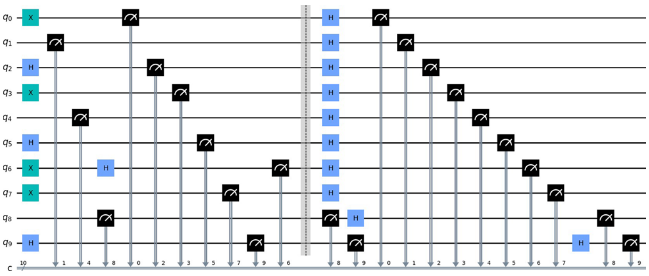
In this study, BB84 protocol served by creating an eavesdropping-resistant quantum cryptographic infrastructure for key protection. IBM Qiskit and Google Cirq served as two main platforms to accomplish this work. The BB84 protocol was designed using IBM Qiskit before Google Cirq executed the testing under realistic noisy conditions including simulated eavesdropping tests.

The evaluation of BB84 protocol required studying two distinct simulation scenarios.

Alice and Bob conducted cryptographic key exchange, which produced an identical key on their respective ends because they experienced no eavesdropping.

Non-eavesdropped communication: In the qubit exchanges between Alice and Bob, the cryptographic keys develop into a perfectly matched key without any form of interception.

Figure 3
Quantum circuit for BB84 protocol



Eavesdropped communication: An attacker named Eve tries to capture qubits, which causes detectable disturbances because of quantum measurement rules.

In an ideal scenario where no adversary interferes, Alice encodes a sequence of qubits using random bases and transmits them to Bob. Bob measures the qubits using his randomly selected bases. After a basic reconciliation over a classical channel, they retain only the qubits where their bases match. As shown in Figure 4, the shared key remains unaltered, demonstrating a 100% key match. This successful exchange ensures a secure cryptographic key for encryption, as Alice's expected key and Bob's actual key are perfectly aligned.

3.2.3. Eavesdropped communication and security analysis

When an adversary (Eve) attempts to intercept the quantum transmission, the no-cloning theorem and quantum measurement disturbance introduce detectable errors in Bob's received qubits. As depicted in Figure 5, this interference disrupts the key agreement process, leading to a mismatch between Alice's expected key and Bob's actual key. To quantify the level of tampering, the error rate Dis computed as:

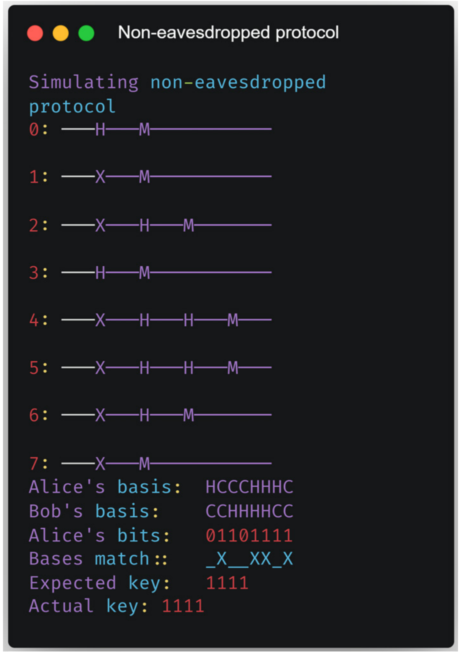
$$\mathrm{D} = \frac{|\textit{discrepant bits}|}{|\textit{total bits}|} \tag{4}$$

Alice and Bob end their communication session at once when the computed error rate (D) exceeds the security threshold because they want to prevent the use of compromised keys for encryption. The BB84 protocol includes a security measure that identifies unapproved access attempts, thereby strengthening its practical worth for quantum cryptographic systems.

3.2.4. Security validation

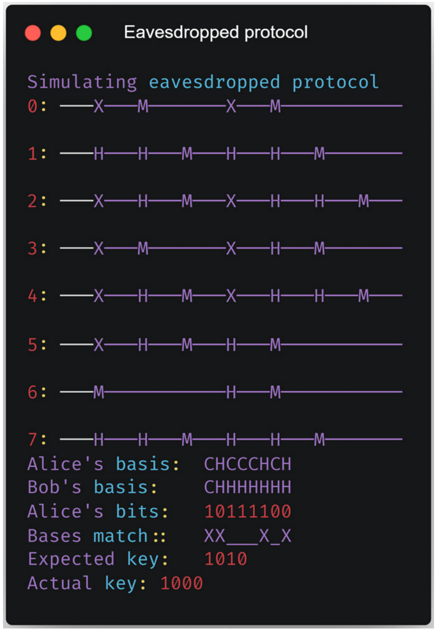
The BB84 protocol establishes its security through two quantum mechanical principles: the no-cloning theorem and measurement disturbance. The no-cloning theorem establishes that an eavesdropper (Eve) cannot generate perfect qubit copies because this process

Figure 4
Non-eavesdropped protocol simulation



```
Simulating non-eavesdropped
protocol
0: ──H──M──────────

1: ──X──M──────────

2: ──X──H──M───────

3: ──H──M──────────

4: ──X──H──H──M──

5: ──X──H──H──M──

6: ──X──H──M───────

7: ──X──M──────────
Alice's basis:   HCCCHHHC
Bob's basis:     CCHHHHCC
Alice's bits:    01101111
Bases match::    _X__XX_X
Expected key:    1111
Actual key: 1111
```

Figure 5
Eavesdropped protocol – Cirq



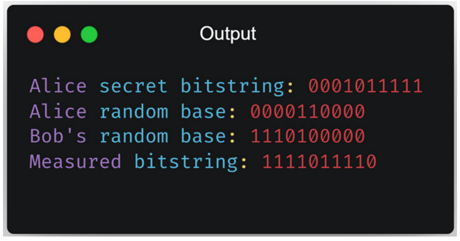
```
Simulating eavesdropped protocol
0: ───X───M───────X───M───────────

1: ───H───H───M───H───H───M───────

2: ───X───H───M───X───H───H───M───

3: ───X───M───────X───H───M───────

4: ───X───H───M───X───H───H───M───

5: ───X───H───M───H───M───────────

6: ───M───────────H───M───────────

7: ───H───H───M───H───H───M───────
Alice's basis:  CHCCCHCH
Bob's basis:    CHHHHHHH
Alice's bits:   10111100
Bases match::   XX___X_X
Expected key:   1010
Actual key: 1000
```

necessarily modifies the original state of the qubit. The process of intercepting and measuring qubits always results in detectable errors that affect the transmission. The protocol implements this feature to detect eavesdropping by removing compromised key sections that exhibit evidence of tampering, thus securing the retained keys.

Simulation outcomes demonstrated that the protocol protected information security throughout both secure and hostile communication situations. The experimental results in Figure 6 show that Alice and Bob successfully generated an aligned shared key because Bob measured identical qubits that Alice sent. When Eve tried to intercept the communication, her actions triggered quantum disturbances that changed the bitstring sent to Bob compared to Alice's original key. When the error rate (D) passed the defined threshold value, the protocol system automatically ended the session to prove its ability for key protection.

While quantum-enabled attacks such as photon number splitting (PNS) and intercept-resend attacks pose potential threats, BB84 remains secure against classical attackers. Decoy state QKD, privacy amplification, and hybrid QKD-PQC encryption architectures are available to improve security and mitigate such threats. Including these techniques in large-scale quantum-safe security implementations should be explored further.

Figure 6
Output of a 10-qubit quantum circuit



```
Alice secret bitstring: 0001011111
Alice random base: 0000110000
Bob's random base: 1110100000
Measured bitstring: 1111011110
```

3.3. Integration of QML models

The BB84 key exchange protocol serves as an important tool in cybersecurity that protects communication pathways by analyzing network behavior irregularities and phishing attacks and harmful URLs. BB84 distributes secure keys by using quantum mechanics principles to implement its operations. Quantum feature maps function as the primary factor behind their success because they create improved data representations that help discover hidden security risks more effectively.

Several features can be represented in parallel by QML models due to quantum superposition, enhancing data representation and reducing training complexity. By establishing feature correlations that classical models find it hard to effectively compute, quantum entanglement strengthens anomaly detection. By making separability nonlinear, quantum feature maps enhance classifiers' capacity for distinguishing between malicious and benign behavior in cybersecurity data.

This work deploys and compares three QML models for cybersecurity use:

1) Variational quantum classifier (VQC)
2) Quantum support vector classifier (QSVC)
3) Quantum neural networks (QNN)

3.3.1. Variational quantum classifier

The VQC uses a combination of quantum computing and classical optimization to resolve classification problems through its three distinct operational stages. The VQC model performs its operations through three fundamental stages can be observed in Algorithm 2.

Algorithm 2: Variational Quantum Classifier (VQC)

```
Input: Training dataset (x,y), feature map Ux, quantum
       circuit Q(θ), learning rate η
Output: Optimized parameters θ*
    1.  Initialize trainable parameters θ for the
        quantum circuit Q(θ).
    2.  For each input data point x:
        a. Encode x into a quantum state:
           |ψ(x)⟩=Ux|0⟩|
        b. Apply the parameterized quantum circuit:
           |ψ′(x,θ)⟩=Q(θ)|ψ(x)⟩
        c. Measure the output probabilities:
           P(y|x,θ)=|⟨y|ψ′(x,θ)⟩|^2
    3.  Compute the loss function (Cross-
        Entropy Loss):
        L(θ)=−y∑ylogP(y|x,θ)
    4.  Update parameters using a classical
        optimizer (e.g., Adam):
                 θ←θ−η∇L(θ)
    5.  Repeat steps 2-4 until convergence.
```

The initial operation starts with quantum feature encoding, which transforms classical input data through specific quantum feature maps $\phi(x)$ to generate quantum states $|\psi(x)\rangle$. The data embedding procedure transforms information into a quantum space with high dimensions, so the model can detect sophisticated patterns that cannot be handled by traditional systems.

$$|\varPsi(x)\rangle = U\phi(x)|0\rangle \tag{5}$$

The quantum state encoding proceeds to an ansatz, which functions as a parameterized quantum circuit θ. During training, the quantum gates with adjustable parameters form the basis of the parameterized quantum circuit. The adjustable parameters in this model structure determine how decision boundaries shape which directly affects the classification accuracy.

The circuit goes through measurement in its last stage to generate output probabilities that correspond to each class label. The measured results are evaluated against actual labels through a loss function. By performing multiple training iterations, a classical optimizer receives feedback that allows it to update circuit parameters ϕ, thereby enhancing model performance.

The VQC implements quantum data encoding functions together with classical optimization algorithms into a unified system. The combination of quantum and classical methods in VQC allows it to find effective solutions for analyzing complex nonlinear data patterns and high-dimensional datasets. The quantum approach with VQC enables superior exploration of feature spaces that leads to better classification results for difficult cases that standard ML methods cannot handle.

3.3.2. Quantum support vector classifier

QSVC executes data transformation through quantum kernels, which create quantum feature space with high dimensions. Fidelity quantum kernel serves as the similarity assessment tool for quantum states during QSVC operation, which enhances its performance in phishing detection because of its ability to detect fine patterns and decision limits.

Quantum kernel function encodes classical data points x, which are encoded into quantum states $|\psi(x)\rangle|$ using a quantum feature map Ux. The similarity between data points in the quantum feature space is represented by the kernel matrix:

$$\mathbf{K}(x_i, x_j) = |\langle \psi(x_i)|\psi(x_j)\rangle|^2 \tag{7}$$

QSVC can identify complex security relationships that standard kernels do not recognize. Training occurs through Pegasos-QSVC implementation and employs stochastic sub-gradient descent as its approach. The regularization parameters C and τ together find the right balance between maximizing margin and preventing overfitting to achieve best results.

The Algorithm 3, QSVC provides effective solutions for high-dimensional datasets because it detects complex relationships that traditional kernel methods fail to detect. The Pegasos optimization algorithm ensures model scalability when dealing with large data volumes during training. Quantum feature mapping united with optimal optimization techniques enables QSVC to outperform conventional classifiers that handle complex and faintly defined data structures.

Algorithm 3: Quantum Support Vector Classifier (QSVC)

```
1. Encode data points x into quantum states $|\psi(x)\rangle$ using the feature map $U_x$.
2. Compute the kernel matrix $K(x_i, x_j) = |\langle\psi(x_i)|\psi(x_j)\rangle|^2$ for all $x_i$, $x_j$ in the dataset.
3. Solve the SVM optimization problem
   Maximize $W(\alpha) = \sum_i \alpha_i - 0.5 \sum_i\sum_j \alpha_i\alpha_j y_i y_j K(x_i, x_j)$,
   Subject to: $0 \le \alpha_i \le C$, $\sum_i \alpha_i y_i = 0$.
4. Compute the decision boundary
   $f(x) = \sum_i \alpha_i y_i K(x_i, x) + b$.
5. Classify new input x_test:
   y_pred = sign(f(x_test)).
```

3.3.3. Quantum neural networks

The QNN improves classical architectures of neural network by incorporating quantum layers so that they can deal with very sophisticated high-dimensional patterns, which traditional ones are not capable of learning. They are useful in tasks like identifying malicious URL, where recognizing hidden relationships and patterns improve classification accuracy. The core of QNN consists of layered quantum gates, which encode data into quantum encoded data and then transform this encoded data to produce a set of feature representations showing nonlinear relationships, which classical methods may fail. This method allows for the most effective training and adaptation of the model with the help of quantum mechanics for the best of the pattern recognition by cybersecurity applications.

Algorithm 4: Quantum Neural Network (QNN)

```
1. Initialize parameters $\theta$ for the quantum circuit $Q(\theta)$.
2. For each input data point x:
   a. Encode x into quantum state $|\psi(x)\rangle$ using $U_x$.
   b. Apply $Q(\theta)$ to $|\psi(x)\rangle$.
   c. Measure the output probabilities $P(y|x, \theta)$.
3. Compute the loss function:
   $L(\theta)$ = Mean squared error $(y, P(y|x, \theta))$.
4. Update parameters $\theta$ using gradient descent:
   $\theta \leftarrow \theta - \eta \nabla L(\theta)$.
5. Repeat steps 2-4 until convergence.
```

The performance of QNN effectively process complex datasets. Quantum computing principles allow QNNs to execute operations in multidimensional spaces, thus making them stand out from other models. QNN helps to identify complex patterns and hidden data beyond traditional neural network detection capabilities. The importance of QNNs increases significantly while performing cybersecurity operations. Their feature detection allows them to discover dangerous URL patterns that conventional networks would not notice.

3.4. Optimization techniques

To enhance the stability and accuracy of QML models, various optimization methods were used. These optimization methods were aimed at suppressing noise in NISQ devices and minimizing the computational expense of quantum kernels. The following strategies were used to enhance classification performance and overall model efficiency.

3.4.1. Noise mitigation

Measurement errors were minimized by quantum circuit output probability calibration, making classification results more accurate. Errors in gates were minimized through randomized execution of circuits, where averaging across several runs reduced the level of inconsistencies created by quantum noise. The observed probability $P_{\text{noisy}}(y|x)$ was corrected using a calibration matrix M, ensuring that the estimated probability $P_{\text{corrected}}(y|x)$ closely aligned with the ideal probability $P_{\text{ideal}}(y|x)$. This noise mitigation strategy enhanced the stability and reliability of QML models in cybersecurity application.

$$P_{\text{corrected}}(y|x) = M^{-1} P_{\text{noisy}}(y|x) \tag{8}$$

Circuits were optimized to reduce gate depth and alleviate decoherence effects, thereby reducing the impact of quantum noise during computations. By executing circuits n times with randomized gates, errors were averaged out, leading to improved computational stability. The denoised estimation of the output probabilities was computed as shown below:

$$\hat{p}(y,x) = \frac{1}{n}\sum_{i=1}^{n} p_{noisy,i}(y|x) \tag{9}$$

where $\hat{p}(y,x)$ is the denoised estimate of the output probabilities.

3.4.2. Custom quantum kernels

Quantum kernels were mainly designed to match the characteristics of the datasets, for phishing detection and malicious URL classification. These kernels transformed classical data into high-dimensional quantum feature spaces, enhancing class separately with reduced computational complexity. Optimization techniques were applied to streamline kernel computations, reducing resource usage while ensuring scalability for handling large-scale cybersecurity datasets.

3.4.3. Hyperparameter tuning

Learning rates were selected to prevent oscillations during parameter updates, ensuring stable training. The number of layers in quantum circuits was optimized to enhance model capability while considering the hardware constraints of NISQ devices. The gradient-based optimization learning rate η was adjusted to ensure smooth convergence:

$$\theta_{t+1} = \theta_t - \eta\, \nabla L(\theta_t) \tag{10}$$

where L(θ) represents the loss function.

Variational ansatz structures, which define the layout of quantum gates, were refined for VQC and QNN models to maximize training efficiency and minimize error propagation.

3.4.4. Hybrid optimization strategies

Classical optimizers were combined with quantum computations for robust parameter tuning. The Adam optimizer was used in gradient-based methods to ensure smooth and rapid convergence for larger datasets, especially in QNN and VQC models.

$$m_t = \beta_1 m_{t-1} + (1 + \beta_1)\, \nabla L(\theta_t) \tag{11}$$

$$v_t = \beta_2 m_{t-1} + (1 + \beta_2)(\,\nabla L(\theta_t))^2 \tag{12}$$

$$\theta_{t+1} = \theta_t - \frac{\eta}{\sqrt{\widehat{V}+\epsilon}}\widehat{m}_t \tag{13}$$

COBYLA was used for models like QSVC to handle non-smooth loss landscapes, which are common in quantum learning tasks. This hybrid approach allows the models to achieve better performance while mitigating the limitations of noisy quantum environments.

$${}^{min}_{\theta}L(\theta), \tag{14}$$

Subject to: $c_j(\theta) \leq 0\ \forall \boldsymbol{j}$.

This ensured robust classification while maintaining the constraints required for cryptographic key validation.

3.4.5. Scalability enhancements

This research implemented optimized ansatz designs for conducting parallel quantum circuit operations, which met computational needs. The flexible approach to quantum hardware design allowed the implemented strategies to boost the efficiency of quantum classification operations. The optimized techniques enhanced performance metrics for accuracy and F1 score across all cybersecurity application tests of QML models.

The experimental results proved that these approaches produced effective results. Noise mitigation techniques produced 20% better accuracy results, and hybrid optimization methods stabilized training through swift convergence with fewer iterations. The quantum kernel development together with parameter optimization was specialized in complex cybersecurity data to achieve additional performance improvements. The proposed optimization framework demonstrates practical use because it achieves successful implementation on current NISQ devices.

Figure 7 depicts a general outline of the QML architecture, showing the combination of data preprocessing, cryptographic security, and quantum-amplified learning models. This framework utilizes QML models like VQC, QSVC, and QNN in combination with quantum-resistant cryptographic protocols to enhance the resilience of cybersecurity. Utilizing cutting-edge preprocessing methods and quantum feature mapping, the approach strengthens anomaly detection on various cybersecurity datasets. Optimization methods further enhance the scalability and efficiency of these models while ensuring their resilience in NISQ settings. Further, incorporating the BB84 protocol allows for a quantum-secure key exchange system with inherent eavesdropping detection, adding strength to security against both classical and quantum cyber threats.

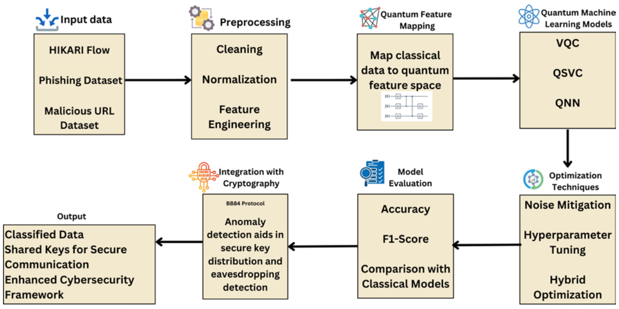
4. Results and Discussion

This section provides the experimental findings of the QML models, evaluating their effectiveness across critical cybersecurity tasks. The discussion about these results within the study's research objectives highlights performance improvements, strengths, and potential challenges.

4.1. Performance evaluation metrics

The QML models received their evaluation using three essential cybersecurity datasets: HIKARI Flow for intrusion detection, phishing, and malicious URL datasets. The evaluation process relied on standard classification metrics, which included precision, recall, F1 score, and accuracy. The evaluation of the model effectiveness in detecting cyber threats can be achieved through the combination of these metrics.

Figure 7
QML architecture



The proportion of actual correct positive cases among all model predictions for positive outcomes demonstrates precision that indicates how well the model performs without creating unjust alarms. The ability of a model to identify genuine threats serves as the focus of recall measurements, which emphasizes its capacity to detect security risks. The F1 metric serves as a balanced performance indicator for models because it computes the precision-recall harmonic mean to evaluate results during unbalanced class problems.

All the evaluation metrics make sure that the strengths and weaknesses of QML models are rigorously measured across various cybersecurity tasks.

4.1.1. Task-specific insights

The section demonstrates the model's performance in specific tasks.

1) The VQC produced a detection accuracy of 95.12% to detect traffic patterns through its utilization of quantum feature maps.
2) The QSVC reached a detection accuracy rate of 97.75% due to quantum kernels, which improved the separation of feature space.
3) The QNN model achieved 95.62% F1 score when identifying malicious URLs through its quantum-enhanced neural layers, which processed high-dimensional data effectively.

The achieved outcomes indicate that QML models present exceptional capabilities for solving advanced cybersecurity problems.

4.2. Comparative analysis

The performance of QML models was evaluated by comparing their results to random forest, gradient boosting, and standard neural networks classical ML algorithms. The QML models delivered superior performance compared with that of classical models during every evaluation task especially when processing high-dimensional datasets to detect complex nonlinear patterns.

The QSVC delivered an outstanding performance in phishing detection through its quantum kernel processing system, which effectively handled intricate datasets; the security datasets used in this study consisted of authentic attack conditions during their evaluation process.

In this study, four cybersecurity datasets that proved their threat validity during testing were evaluated.

1) The HIKARI Flow dataset serves as a dataset that mixes both encrypted synthetic attack traffic and benign network flows to assist intrusion detection tasks.
2) The phishing dataset unites parameters extracted from network systems with email metadata components and links each entry to phishing or legitimate status.
3) The Malicious URL dataset consists of a collection of malicious URLs, which security analysts commonly used for threat analysis.

4.3. Performance on HIKARI Flow dataset

The HIKARI Flow dataset, which is employed for intrusion detection, was evaluated using several traditional ML models to create a performance baseline. Among those, the Decision Tree classifiers and gradient boosting performed well, with near-perfect accuracy. Their high performance is due to their capacity for modeling nonlinear relationships and the detection of less apparent patterns in network traffic. Naive Bayes, on the other hand, performed poorly because of the feature independence assumption. The high-dimensionality of the dataset and correlated dependencies between features complicated the classification of network traffic by Naive Bayes. From Figure 8, ensemble-driven models outperformed the rest consistently, reflecting their capability to tackle complex intrusion detection processes. These findings point to the inadequacies of traditional classifiers in dealing with intricate network traffic, affirming the necessity of QML models that utilize quantum feature spaces for improved classification accuracy and scalability.

4.3.1. Performance on Phishing dataset (network parameters)

For network parameter-based phishing detection, traditional ML algorithms like gradient boosting and random forest performed with highest accuracy and improved further through hyperparameter tuning, making gradient boosting the best classifier for this data. Figure 9 indicates that ensemble models like gradient boosting and random forest performed the best at every time point in phishing classification. In contrast, Naive Bayes did not perform well because it could not accurately depict feature dependencies, which are essential in detecting phishing patterns. These results highlight the weakness of probabilistic models for phishing detection, further confirming the need for QML models that utilize quantum-boosted kernels to enhance feature separability and accuracy in classification.

4.4. Performance on phishing dataset (email content)

For email content-based phishing detection, powerful ensemble classifiers like CatBoost and XGBoost (XGB) proved to be the best, with accuracy rates over 98%. These models were able to capture fine differences in phishing emails, rendering them extremely robust for classification. As shown in Figure 10, ensemble models like extra trees and random forest proved to be the most effective in phishing

Figure 8
Performance of classical models on HIKARI Flow dataset

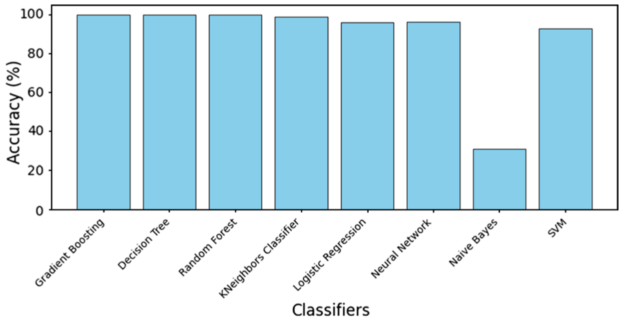


Figure 9
Performance of classical models on phishing dataset (network parameters)

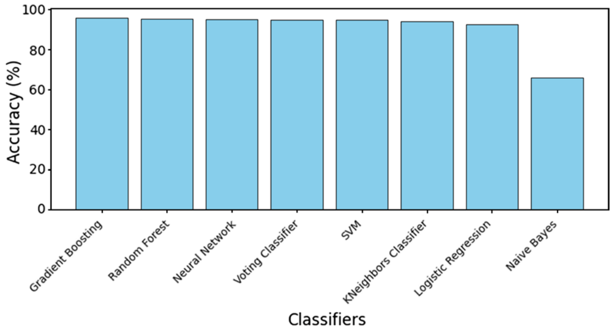
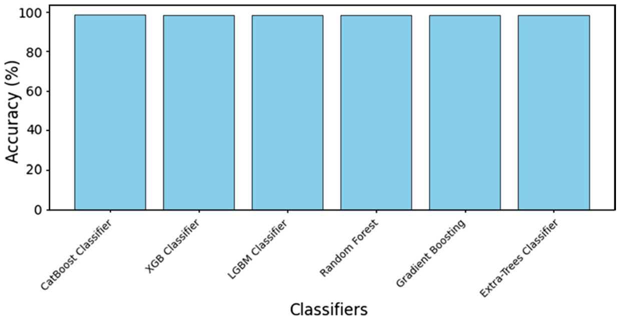


Figure 10
Performance of classical models on phishing dataset (email content)



email detection, utilizing heterogeneous decision trees for better generalization. Conversely, Gaussian Naive Bayes underperformed because it is based on naive probabilistic assumptions, which are not as effective at modeling the intricate structures and relationships present in phishing email datasets. These findings emphasize the strengths of ensemble learning for phishing detection and support the potential of QML models to further improve classification accuracy by applying quantum feature mapping methods.

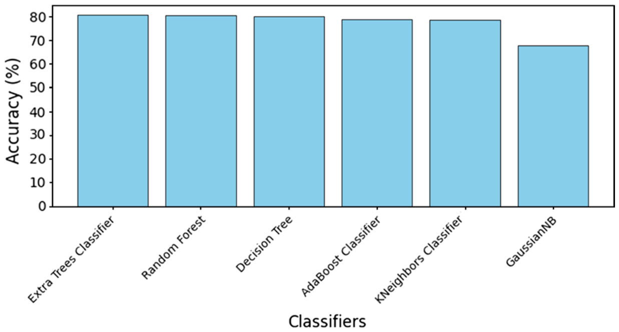
4.5. Performance on Malicious URL dataset

For the malicious URL classification task, extra trees and random forest were the leading classical models that provided the highest accuracy and F1 scores. The ensemble-based classifiers are very efficient at capturing intricate patterns in the dataset and were consequently very reliable at classifying malicious URLs. CatBoost and XGB also proved very effective at the classification task, as can be seen from Figure 11, by utilizing gradient boosting to improve decision boundaries. Random forest and extra trees also confirmed their strength by accurately separating benign and malicious URLs. The results emphasize the efficiency of ensemble models in URL classification and the potential of QML models to further improve detection using quantum-improved feature mapping and kernel-based separability.

4.6. Comparison with QML models

Results showed that the QML model performed better than traditional ML approaches across all examined datasets with consistent results. Quantum feature mapping in high dimensions enabled their effective operational capability, which resulted in better cybersecurity threat detection capabilities. The quantitative results from the QML assessment showed that QSVC delivered the best outcomes with an average output accuracy of 97.75%. Phishing and malicious URL detection tasks benefited greatly from quantum kernels because they produced better class separability, which led to improved performance.

Figure 11
Performance of classical models on Malicious URL dataset



The core model architecture of QML models received essential support from various optimization techniques that improved both accuracy and model resistance. The development process included fine-tuning hyperparameters along with suitable noise mitigation techniques for NISQ hardware and adaptive kernel configuration implementation. The listed improvements in Table 2 delivered enhanced precision and robustness to the proposed security framework based on QML while surpassing traditional methods.

As shown in Table 2, optimization techniques, including hyperparameter tuning and noise mitigation, significantly improved the performance of QML models. VQC and quantum convolutional neural network achieved near-perfect scores in most tasks, highlighting the effectiveness of optimization in enhancing quantum model.

Table 2
Performance of QML models before and after optimization across datasets

Dataset	QML model	Score before optimization	Score after optimization
HIKARI Flow	Variational quantum classifier	0.64	0.99
	Quantum support vector classifier	0.53	0.97
	Quantum neural network	0.78	0.95
	QSVC with Pegasos algorithm	0.63	0.98
	Quantum convolutional neural network	0.57	0.99
Phishing (email content)	Variational quantum classifier	0.61	0.97
	Quantum support vector classifier	0.66	0.98
	Quantum neural network	0.67	0.93
	QSVC with Pegasos algorithm	0.59	0.98
	Quantum convolutional neural network	0.68	0.99
Phishing (network parameters)	Variational quantum classifier	0.66	0.96
	Quantum support vector classifier	0.79	0.96
	Quantum neural network	0.69	0.99
	QSVC with Pegasos algorithm	0.57	0.89
	Quantum convolutional neural network	0.79	0.94
Malicious URL	Variational quantum classifier	0.73	0.99
	Quantum support vector classifier	0.77	0.96
	Quantum neural network	0.65	0.99
	QSVC with Pegasos algorithm	0.65	0.97
	Quantum convolutional neural network	0.73	0.94

The results in Figure 12 confirm the advantage of QML models over classical approaches in handling high-dimensional datasets. The enhanced capability of QML models in quantum-safe cryptographic frameworks highlights their potential for future advancements in cybersecurity applications.

4.7. Discussion

The study proves that QML models perform better than traditional cybersecurity methods. The models tested their ability to detect intrusion attacks, phishing threats and malicious URLs. The QSVC obtained the best results with 97.75% average accuracy during phishing detection tasks. The quantum kernel technology delivers strong performance in phishing detection because it effectively separated classes for identifying subtle distinctions in phishing data. The VQC and QNN achieved competitive results by detecting intrusions and malicious URLs. Through quantum techniques, these systems achieved superior capabilities to find hidden patterns and this advantage gave them an advantage over traditional ML models.

Optimization methods were necessary in improving model performance. Before optimization, QML models were hindered by noise in quantum computation, which reduced accuracy. Further the implementation of methods like the reduction of noise, hyperparameter adjustment, and enhancement of circuit design, the models witnessed a good improvement in accuracy. In Table 2, both the VQC and QNN achieved near-perfect accuracy upon optimization, which confirms the efficiency of quantum error correction approaches.

When comparing QML and traditional ML approaches, clear advantages were observed. Classical models like gradient boosting and random forest performed well when working with structured datasets that had fewer feature dependencies. However, these models struggled with datasets containing complex relationships between features. In phishing detection using email content, for example, the QSVC outperformed gradient boosting, achieving an accuracy of 98.75%. This reveals the power of quantum-enhanced feature processing, which can capture complex relationships that classical methods might not.

Although these results are promising, there still exists significant hurdles in the real-world implementation of quantum-enhanced cybersecurity infrastructures. For heuristic methods, current quantum devices are at the NISQ era, with current devices having noisiness that introduces inconsistency during the training phase. Moreover, quantum kernel methods carry computationally intensive resources, making it challenging for large-scale implementations. Table 3 highlights these challenges alongside possible data mitigation strategies.

Figure 12
Average performance of quantum models

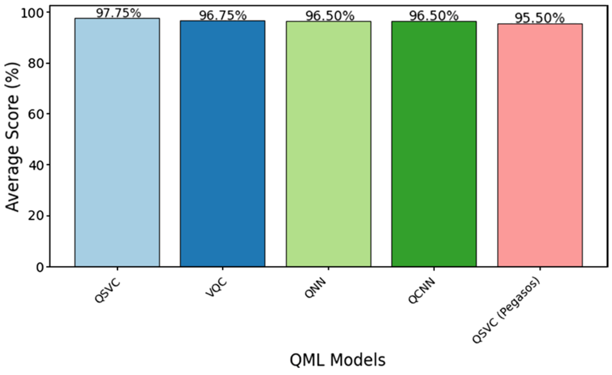


Table 3
Challenges in adopting quantum-safe cybersecurity

Challenge	Description	Impact	Potential solutions
Hardware limitations [20]	Limited qubits and high error rates in NISQ cause instability	Unreliable computations and unstable QKD	Error correction, noise mitigation, and hybrid quantum-classical models
Lack of standardization [32]	No universal PQC and QKD protocols hinder uniform deployment	Capability issues with existing systems	Global standard and hybrid encryption
Integration with existing security systems [41]	QML and QKD protocols do not easily work with classical security	Hard to switch from classical to quantum security	Development of Quantum-safe Transport Layer Security (TLS) and middleware solutions
Computational and energy costs [37]	Quantum hardware requires lot of cooling	Expensive and hard to scale	Energy-efficient photonic processors

Three main strategic developments are required for solving current challenges involving quantum hardware improvements, quantum noise control and hybrid quantum-classical system design (Table 3). System stability and application scalability will be achieved through the required system enhancements. System security protection against threats represents the main purpose in quantum-safe cybersecurity. Scientists protect sensitive quantum model-processed data by implementing FHE as a privacy-protecting method; this framework should be applied to existing applications. Research on quantum security requires both enhanced error correction protocols and optimized techniques, as well as improved QML security systems for real-world implementation.

5. Conclusion

Quantum computing continues to evolve quickly, which exposes security threats to the cybersecurity domain. Cryptography using traditional mathematical algorithms becomes weaker during the quantum development of new computing algorithms. Research on quantum-secure cybersecurity methods has gained high priority due to the current security environment. This framework was developed by merging BB84 QKD protocol with QML models to secure the data more effectively.

The study shows that QSVC, together with VQC and QNN, surpassed classical ML models across all cybersecurity operations. This performs three cybersecurity operations: intrusion detection, phishing classification, and malicious URL detection. The QSVC achieved the highest accuracy rate of 97.75% for phishing detection. The accuracy of classification improves through quantum feature representations, which enable better distinction between genuine and malicious activity. The model performance received significant improvements from optimization techniques that included quantum kernel adjustment and noise removal, and hyperparameter tuning. The current limitations of quantum hardware do not reduce the fact that QML proves itself as an effective cybersecurity solution.

Research work in the field should concentrate on developing QML models that can process advanced cybersecurity datasets with larger dimensions. The main obstacle in quantum kernel methods is to minimize their computational requirements for better performance. This study focuses on integrating QML with PQC protocols to enhance the security system that defends against both classical and quantum threats. Hybrid quantum-classical models serve as a solution to achieve the best combination of computational speed and quantum learning advantages. Real-world cybersecurity infrastructure implementations of these models will be essential for assessing their operational effectiveness under dynamic and evolving cyber threat conditions.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data are available from the corresponding author upon reasonable request.

Author Contribution Statement

Ramasubramaniyan Gunasridharan: Methodology. **Ali Altalbe:** Methodology. **Bharathi Mohan Gurusamy:** Conceptualization, Writing - review & editing. **Gundala Pallavi:** Writing - original draft. **Prasanna Kumar Rangarajan:** Supervision.

References

[1] Chawla, D., & Mehra, P. S. (2023). A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions. *Internet of Things*, *24*, 100950. https://doi.org/10.1016/j.iot.2023.100950

[2] Barbeau, M., & Garcia-Alfaro, J. (2022). Cyber-physical defense in the quantum era. *Scientific Reports*, *12*(1), 1905. https://doi.org/10.1038/s41598-022-05690-1

[3] Fitzgibbon, G., & Ottaviani, C. (2024). Constrained device performance benchmarking with the implementation of post-quantum cryptography. *Cryptography*, *8*(2), 21. https://doi.org/10.3390/cryptography8020021

[4] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

[5] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. In *2018 10th International Conference on Cyber Conflict*, 371–390. https://doi.org/10.23919/CYCON.2018.8405026

[6] Aïmeur, E., Brassard, G., & Gambs, S. (2013). Quantum speed-up for unsupervised learning. *Machine Learning*, *90*(2), 261–287. https://doi.org/10.1007/s10994-012-5316-5

[7] Bernstein, D. J. (2024). Cryptographic competitions. *Journal of Cryptology*, *37*(1), 7. https://doi.org/10.1007/s00145-023-09467-1

[8] Radanliev, P. (2024). Artificial intelligence and quantum cryptography. *Journal of Analytical Science and Technology*, *15*(1), 4. https://doi.org/10.1186/s40543-024-00416-6

[9] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

[10] Das, R., & Sandhane, R. (2021). Artificial intelligence in cyber security. *Journal of Physics: Conference Series*, *1964*(4),1742–042072. https://doi.org/10.1088/1742-6596/1964/4/042072

[11] Sehgal, S. K., & Gupta, R. (2021). Quantum cryptography and quantum key. In *2021 International Conference on Industrial Electronics Research and Applications*, 1–5. https://doi.org/10.1109/ICIERA53202.2021.9726722

[12] Rios Insua, D., Naveiro, R., Gallego, V., & Poulos, J. (2023). Adversarial machine learning: Bayesian perspectives. *Journal of the American Statistical Association*, *118*(543), 2195–2206. https://doi.org/10.1080/01621459.2023.2183129

[13] Avro, S. S., Rahman, S. A., Tseng, T. L. B., & Rahman, M. F. (2024). A deep learning framework for automated anomaly detection and localization in fused filament fabrication. *Manufacturing Letters*, *41*, 1526–1534. https://doi.org/10.1016/j.mfglet.2024.09.179

[14] Okeke, K., & Omojola, S. (2025). Enhancing cybersecurity measures in critical infrastructure: Challenges and innovations for resilience. *Journal of Scientific Research and Reports*, *31*(2), 474–484. https://dx.doi.org/10.9734/jsrr/2025/v31i22868

[15] Thakur, K., Ali, M. L., Obaidat, M. A., & Kamruzzaman, A. (2023). A systematic review on deep-learning-based phishing email detection. *Electronics*, *12*(21), 4545. https://doi.org/10.3390/electronics12214545

[16] Nag, Y. M., Hullatti, V. M., Aiyappa, T. B., & Kher, U. (2024). Ethical concerns of using artificial intelligence in cybersecurity. *International Journal of Advanced Research in Computer and Communication Engineering*, *13*(11), 243–246. https://doi.org/10.17148/IJARCCE.2024.131138

[17] Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S. (2017). Quantum machine learning. *Nature*, *549*(7671), 195–202. https://doi.org/10.1038/nature23474

[18] Schuld, M., Sinayskiy, I., & Petruccione, F. (2015). An introduction to quantum machine learning. *Contemporary Physics*, *56*(2), 172–185. https://doi.org/10.1080/00107514.2014.964942

[19] Akter, M. S., Shahriar, H., Ahamed, S. I., Gupta, K. D., Rahman, M., Mohamed, A., ..., & Wu, F. (2023). Case study-based approach of quantum machine learning in cybersecurity: Quantum support vector machine for malware classification and protection. In *2023 IEEE 47th Annual Computers, Software, and Applications Conference*, 1057–1063. https://doi.org/10.1109/COMPSAC57700.2023.00161

[20] Rosa-Remedios, C., & Caballero-Gil, P. (2025). Optimizing quantum machine learning for proactive cybersecurity. *Optimization and Engineering*, *26*(4), 2321–2353. https://doi.org/10.1007/s11081-024-09934-z

[21] Abreu, D., Rothenberg, C. E., & Abelém, A. (2024). QML-IDS: Quantum machine learning intrusion detection system. In *2024 IEEE Symposium on Computers and Communications*, 1–6. https://doi.org/10.1109/ISCC61673.2024.10733655

[22] Ciliberto, C., Herbster, M., Ialongo, A. D., Pontil, M., Rocchetto, A., Severini, S., & Wossnig, L. (2018). Quantum machine learning: A classical perspective. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *474*(2209), 20170551. https://doi.org/10.1098/rspa.2017.0551

[23] Rahman, M. A., Akter, M. S., Miller, E., Timofti, B., Shahriar, H., Masum, M., & Wu, F. (2024). 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*, 1067–1072. https://doi.org/10.1109/COMPSAC61105.2024.00144

[24] Ciaramella, G., Iadarola, G., Mercaldo, F., Storto, M., Santone, A., & Martinelli, F. (2022). Introducing quantum computing in mobile malware detection. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 88. https://doi.org/10.1145/3538969.3543816

[25] Kalinin, M., & Krundyshev, V. (2023). Security intrusion detection using quantum machine learning techniques. *Journal of Computer Virology and Hacking Techniques*, *19*(1), 125–136. https://doi.org/10.1007/s11416-022-00435-0

[26] Acín, A., Brunner, N., Gisin, N., Massar, S., Pironio, S., & Scarani, V. (2007). Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, *98*(23), 230501. https://doi.org/10.1103/PhysRevLett.98.230501

[27] Reddy, S., Mandal, S., & Mohan, C. (2023). Comprehensive study of BB84, a quantum key distribution protocol. *International Research Journal of Engineering and Technology*, *10*(3), 1023–1034.

[28] Bloom, Y., Fields, I., Maslennikov, A., & Rozenman, G. G. (2022). Quantum cryptography—A simplified undergraduate experiment and simulation. *Physics*, *4*(1), 104–123. https://doi.org/10.3390/physics4010009

[29] Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, *560*, 7–11. https://doi.org/10.1016/j.tcs.2014.05.025

[30] Khan, S., Zheng, J., Ullah, F., Akhter, M. P., Khan, S., Awwad, F. A., & Ismail, E. A. (2024). Hybrid computing framework security in dynamic offloading for IoT-enabled smart home system. *PeerJ Computer Science*, *10*, e2211. https://doi.org/10.7717/peerj-cs.2211

[31] Majid, B., Sofi, S. A., & Jabeen, Z. (2025). Quantum machine learning: A systematic categorization based on learning paradigms, NISQ suitability, and fault tolerance. *Quantum Machine Intelligence*, *7*(1), 39. https://doi.org/10.1007/s42484-025-00266-4

[32] Li, C., Kumar, N., Song, Z., Chakrabarti, S., & Pistoia, M. (2024). Privacy-preserving quantum federated learning via gradient hiding. *Quantum Science and Technology*, *9*(3), 035028. https://doi.org/10.1088/2058-9565/ad40cc

[33] Dash, B., & Ullah, S. (2024). Quantum-safe: Cybersecurity in the age of quantum-powered AI. *World Journal of Advanced Research and Reviews*, *21*(1), 1555–1563. https://doi.org/10.30574/wjarr.2024.21.1.2640

[34] Wang, Z., Luo, N., & Zhou, P. (2020). GuardHealth: Blockchain empowered secure data management and Graph Convolutional Network enabled anomaly detection in smart healthcare. *Journal of Parallel and Distributed Computing*, *142*, 1–12. https://doi.org/10.1016/j.jpdc.2020.03.004

[35] Szymanski, T. H. (2024). A quantum-safe software-defined deterministic Internet of Things (IoT) with hardware-enforced cyber-security for critical infrastructures. *Information*, *15*(4), 173. https://doi.org/10.3390/info15040173

[36] Rencis, E., Vīksna, J., Kozlovičs, S., Celms, E., Lāriņš, D. J., & Petručeņa, K. (2024). Hybrid QKD-based framework for secure enterprise communication system. *Procedia Computer Science*, *239*, 420–428. https://doi.org/10.1016/j.procs.2024.06.189

[37] Fedorov, A. K. (2023). Deploying hybrid quantum-secured infrastructure for applications: When quantum and post-quantum can work together. *Frontiers in Quantum Science and Technology*, *2*, 1164428. https://doi.org/10.3389/frqst.2023.1164428

[38] Hasmitha Krishna, N., Sridevi, S., & Prasanna Kumar, R. (2023). Quantum kernel-aided support vector machine classifier for improved speech classification. In *2023 14th International Conference on Computing Communication and Networking Technologies*, 1–6. https://doi.org/10.1109/ICCCNT56998.2023.10307618

[39] Awasthi, A. (2025). The role of quantum machine learning in cybersecurity. *International Research Journal of Modernization in Engineering Technology and Science*, *7*(1), 5223–5228.

[40] Tehrani, M. G., Sultanow, E., Buchanan, W. J., Amir, M., Jeschke, A., Houmani, M., ..., & Lemoudden, M. (2024). Stabilized quantum-enhanced SIEM architecture and speed-up through Hoeffding tree algorithms enable quantum cybersecurity analytics in botnet detection. *Scientific Reports*, *14*(1), 1732. https://doi.org/10.1038/s41598-024-51941-8

[41] Radanliev, P., de Roure, D., & Santos, O. (2023). *Red Teaming Generative AI/NLP, the BB84 quantum cryptography protocol and the NIST-approved Quantum-Resistant Cryptographic Algorithms*. arXiv. https://doi.org/10.48550/arXiv.2310.04425

[42] Bellante, A., Fioravanti, T., Carminati, M., Zanero, S., & Luongo, A. (2025). Evaluating the potential of quantum machine learning in cybersecurity: A case-study on PCA-based intrusion detection systems. *Computers & Security*, *154*, 104341. https://doi.org/10.1016/j.cose.2025.104341

[43] Farouk, A., Al-Kuwari, S., Abulkasim, H., Mumtaz, S., Adil, M., & Song, H. (2025). Quantum computing: A tool for zero-trust wireless networks. *IEEE Network*, *39*(1), 140–148. https://doi.org/10.1109/MNET.2024.3420166

How to Cite: Gunasridharan, R., Altalbe, A., Gurusamy, B. M., Pallavi, G., & Rangarajan, P. K. (2026). A Hybrid Framework Integrating QML, AI, and Quantum-Safe Cryptography for Cybersecurity. *Journal of Computational and Cognitive Engineering*, *5*(1), 16–29. https://doi.org/10.47852/bonviewJCCE52025121

Appendix

Glossary of Acronyms
BB84: Bennett-Brassard 1984 protocol for Quantum Key Distribution
VQC: Variational quantum classifier
QSVC: Quantum support vector classifier
QNN: Quantum neural network
NISQ: Noisy intermediate-scale quantum
ML: machine learning
AI: artificial intelligence
ECC: elliptic curve cryptography
QKD: quantum key distribution
QML: quantum machine learning
IDS: intrusion detection systems
COBYLA: Constrained Optimization By Linear Approximations
QCNN: Quantum convolutional neural network