Date of publication 14/09/2022, date of current version 14/09/2022.

VECTORAL manuscript Identifier 14.01-5/VECTORAL.2022.PUB

APPLICATIONS OF QUANTUM COMPUTING IN TELECOM E-COMMERCE: ANALYSIS OF QKD, QAOA, AND QML FOR DATA ENCRYPTION, SPEED OPTIMIZATION, AND AI-DRIVEN CUSTOMER EXPERIENCE

RAHUL KHURANA [1]

[1] Bothell, WA, USA

Corresponding author: Khurana, R.

ABSTRACT Quantum computing methods take advantage of the principles of superposition and entanglement to facilitate parallel computing that is beyond the reach of classical systems. These advances have implications for the telecommunications e-commerce industry because the sector demands secure data transmission, optimal resource allocation, and analysis of huge volumes of data. It reviews three important applications of quantum computing in this domain: *Quantum Key Distribution (QKD), the Quantum Approximate Optimization Algorithm (QAOA), and quantum machine learning (QML)*. QKD makes data more secure by using quantum states that will allow keys to be exchanged securely and make it resistant to quantum attacks against classical encryption. QAOA is reviewed for their potential to solve network traffic management and resource allocation to ensure computational time reduction and network efficiency enhancement. QML is also discussed with its role in processing high-dimensi]onal customer data to optimize the capability of predictive analytics and customer behavior analysis using quantum-enhanced models. The other issues tackled in the study involve qubit decoherence, the requirement for quantum error correction, and integration with quantum-classical systems. We argue here that these challenges need to be solved for practical deployment of quantum computing in telecom applications. Our findings suggest that meeting full-scale implementation will require these barriers.

INDEX TERMS clinical decision-making, data integrity, data pipelines, healthcare data management, HIPAA compliance, IoT data integration, ETL process

I. INTRODUCTION

Quantum computing is based on the principles of superposition and entanglement; it allows qubits or quantum bits to handle information quite differently from the way classical bits operate (Bennett et al., 1997; DiVincenzo, 1995). A qubit can be mathematically represented as $\alpha|0\rangle + \beta|1\rangle$, enables complex information encoding through coefficients α and β, where $|\alpha|^2 + |\beta|^2 = 1$. Because of the superposition that allows quantum systems to represent many states at once, the resultant state space becomes exponentially bigger in comparison with classical systems. When several qubits become entangled, their states become interrelated in such a way that the measurement of one immediately influences the results of measurements of the others, independently of how distant they are. This property enables better efficiency in coordination at different computational processes (Gruska et al., 1999; Williams, 2010).

Shor's algorithm is one of the simplest examples of how quantum mechanics can solve a problem that has been regarded as intractable by a classical computer (Bennett et al., 1997; Kitaev et al., 2002). It factors large integers in polynomial time by making use of the Quantum Fourier Transform, which is an essential step to uncover periodicity in functions. The QFT operation can be defined as:

$$QFT(|x\rangle) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ikx/N} |k\rangle,$$

where it transforms the given state to a superposition encoding the structure of the function under consideration. That transformation drastically reduces the computational complexity of integer factorization to one of $O((\log N)^3)$, from exponential time taken classically. The reduction of the complexity classes has implications for cryptography: the security of popular encryption schemes like RSA depends on the hardness of factoring large numbers.

Another recent and significant contribution of quantum computing is Grover's algorithm, which performs search on unstructured databases with a quadratic speedup. Classically, the process of searching for an element from among N items takes $O(N)$ queries, while Grover's algorithm accomplishes this in $O(\sqrt{N})$ time. This uses the Grover diffusion operator given as $G = 2|\psi\rangle\langle\psi| - I$, where $|\psi\rangle$ is the superposition of all possible states and I is the identity matrix; this effectively amplifies the probability of the correct answer so that it can appear upon measurement. A mechanism like this, even more in general, is helpful not only for database searching but also for optimization problems in general, where such a capability of the algorithm to efficiently explore possible solutions can be applied (Knill, 2005; Ladd et al., 2010).

Quantum systems currently work within the NISQ paradigm, in which the devices are featured by limited coherence times and being very susceptible to noise. Quantum coherence is a sensitive issue because interactions with the environment might cause errors that collapse a qubit superposition state into a classical one. The decoherence processes are quantified with parameters such as T_1, being the energy relaxation time, and T_2, being the phase coherence time. These constraints have consequences on the reliability of quantum computations; hence, methods to mitigate noise have to be elaborated, such as quantum error correction. QEC methods have theoretical promise but come at a significant cost of great resources, constant maintenance, and a tremendous overhead of physical qubits for the stability of even just one logical qubit.

The hardware for quantum computation is manifold, each with specific benefits and limitations. Superconducting qubits use Josephson junctions, which maintain their quantum states at extremely low temperatures, though face challenges due to coherence times and fabrication. Trapped ion qubits are ions held together by electromagnetic fields, offering longer coherence times, while their manipulation—also by lasers to perform operations—means gate speeds are much slower. Photonic systems operate on light particles, hence the speed at which operations can be carried out is faster, although at the cost of losses in the photons, and challenges around integration. These hardware platforms correspond to different approaches in the management of physical difficulties accompanying the implementation of quantum computation, with active research ongoing to improve stability and scalability (Preskill, 2018; Weber et al., 2010).

In general, the implementation of quantum algorithms contains three steps: data loading, computation, and measurement. The preparation of quantum states at this data loading phase is a non-trivial challenge, as classical data has to be encoded into quantum states in such a way that useful information is preserved. In the computation step, quantum circuits manipulate these states via a sequence of quantum gates. In this way, the Hadamard gate is used to prepare an equal superposition of qubit states, which is generally represented as $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Such transforms provide quantum systems with the capability to process information in parallel (McMahon, 2008; Nielsen & Chuang, 2001). Then by measurement, the quantum state collapses into a specific classical outcome, thus converting quantum information back into an exploitable classical form. Since quantum measurement is a probabilistic process, several runs of the algorithm might be needed to obtain a correct answer.

Quantum computing has cryptanalytic implications because it allows one to solve many problems efficiently that are at the heart of classical cryptographic systems. Quantum algorithms, such as Shor's algorithm, could factor large integers in polynomial time, which would grossly compromise the security of many public-key cryptosystems used today, such as RSA. Resulting from this is the research into post-quantum cryptographic methods designed to be resistant to attacks by quantum computers. One of the promising approaches to solve this problem is lattice-based cryptography, because it is believed to resist the powers of quantum computation. On the other hand, quantum key distribution makes use of principles of quantum mechanics such as the no-cloning theorem and uncertainty principle to develop secure communication channels that can detect any eavesdropping attempt (Steane, 1998; Weber et al., 2010).

II. BACKGROUND

Quantum computing is based on a number of basic principles that differ from classical computing. First, the most basic unit of quantum information is called a qubit. It can be thought of as a vector in a two-dimensional complex vector space. The two standard basis states $|0\rangle$ and $|1\rangle$ can be written as:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

The general qubit state has the form given as a superposition of these basis states, and mathematically it may be written as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

where the coefficients α and β are complex numbers subject to the constraint that $|\alpha|^2 + |\beta|^2 = 1$, ensuring that the probability of measuring the qubit in either state $|0\rangle$ or $|1\rangle$ sums to 1.

Another fundamental principle governing quantum information is entanglement. For a system of two or more qubits, the state of one depends on that of the other (Knill, 2005; Nielsen & Chuang, 2010). Perhaps the best-known example of such a two-qubit entangled state is the so-called Bell state:

TABLE 1. Key Quantum Computing Algorithms and Their Complexity

Algorithm	Classical Complexity	Quantum Complexity
Shor's Algorithm	Exponential (e.g., RSA with 2^n complexity)	Polynomial $O((\log N)^3)$ for factoring N
Grover's Algorithm	$O(N)$ for unstructured search	$O(\sqrt{N})$
Quantum Fourier Transform (QFT)	$O(n \log n)$	$O(\log^2 n)$
Variational Quantum Eigensolver (VQE)	Depends on problem size	Dependent on quantum circuit depth and number of shots

TABLE 2. Comparison of Quantum Hardware Platforms

Platform	Qubit Technology	Challenges
Superconducting Qubits	Josephson junction-based circuits	Decoherence, limited connectivity, and fabrication complexity
Trapped Ions	Ion traps manipulated by lasers	Slow gate speeds, cooling requirements
Photonic Systems	Light-based qubits	Photon loss, difficult integration with other qubit types
Topological Qubits	Non-Abelian anyons	High error resistance but still in early research stages

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}.$$

In this form, the combined state cannot be separated into individual states of each qubit, implying that if you measure the state of one qubit, you affect the state of the other.

Quantum interference plays a very important role in quantum algorithms, where probability amplitudes of quantum states interfere to enhance the probability of correct outcomes while suppressing the probability of incorrect outcomes (McMahon, 2008; O'brien, 2007). This is achieved by the application of unitary transformations, which are matrices acting on quantum states. For example, the Hadamard gate, which creates equal superpositions, is given by

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}.$$

We apply the Hadamard gate to $|0\rangle$:

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix},$$

which creates a superposition with equal probability amplitudes for both $|0\rangle$ and $|1\rangle$.

III. DATA ENCRYPTION THROUGH QUANTUM TECHNIQUES

Quantum Key Distribution, in short QKD, uses the key principles of quantum mechanics to enable secure encryption key exchange via quantum channels in telecommunication commerce. One of the bases of this area is the protocol known as the BB84, which encodes binary data into polarized photons to avail the physical principle that a quantum state is perturbed by measurement. In this scheme, Alice generates a string of random bits and assigns each bit to a polarization basis-again, random-rectilinear or diagonal. Arbitrarily, one could decide that a 0 is encoded as a horizontally polarized photon in the case of a rectilinear basis, while 1 is encoded as a vertically polarized photon. She sends these photons through a quantum channel to Bob, who, without knowing Alice's basis choice, chooses an independent measurement basis for each incoming photon (Bova et al., 2021).

As Bob measures the received photons, he correctly identifies the bit value when his basis choice coincides with Alice's. Where the bases differ, the measurement results get randomized, and such bits are subsequently discarded by Bob. For the sifting process, Alice and Bob classically discuss on what bases they prepared the states with, not revealing the actual bit values. This would give them a raw key of those bits where their choice of basis matched. Due to the fact that any eavesdropper, Eve, would necessarily perturb the quantum states of the photons, when trying to measure them, detectable anomalies would have been introduced into the key (Fisher et al., 2014; Gong et al., 2020).

A central part of QKD in telecommunication is the analysis of error rates to detect eavesdropping. Alice and Bob use a subset of their shared bits to estimate the quantum bit error rate (QBER), defined as the ratio between mismatched bits and the total tested bits. A high QBER indicates interference, as the measurements performed by Eve introduce mismatches between the original bit values held by Alice and those measured by Bob. This is an important step in estimation to keep the residuary key intact, guiding further processes such as error correction and privacy amplification to determine a secure key for use in cryptographic applications (Gruska et al., 1999; Hassija et al., 2020).

An effective secure key rate R_{sec} is obtained by correcting the raw key rate R_{raw} due to the occurrence of these errors and the necessary privacy provided. It is approximated by:

$$R_{\text{sec}} = R_{\text{raw}}\left(1 - 2H_2(Q)\right),$$

where $H_2(Q)$ is the binary entropy function, defined as $H_2(Q) = -Q\log_2(Q) - (1-Q)\log_2(1-Q)$, and Q denotes the QBER. The binary entropy function essentially captures the uncertainty of the errors. A lower QBER directly implies

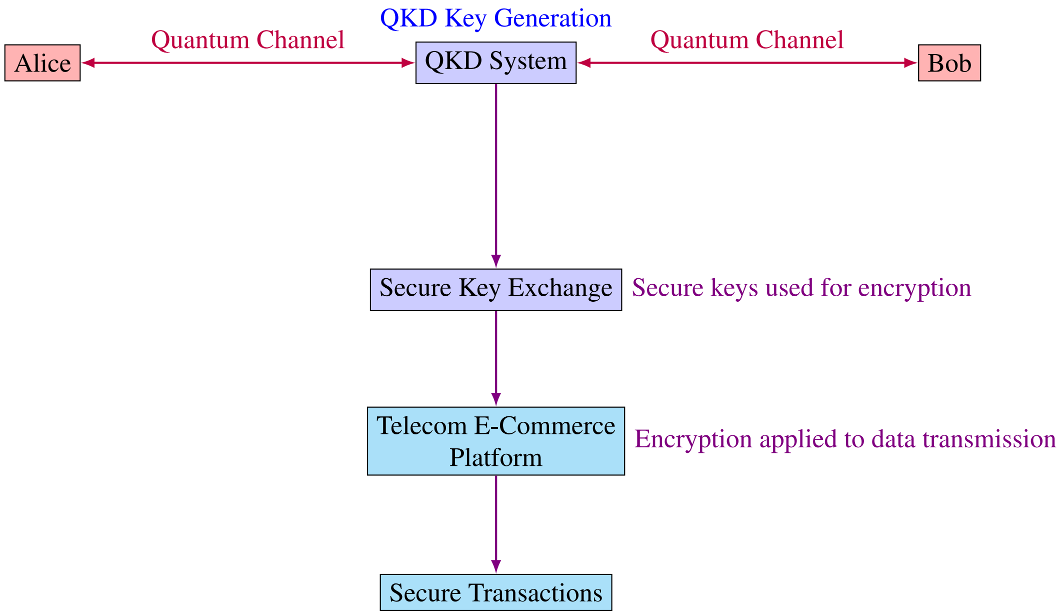

FIGURE 1. Integration of QKD in Telecom E-Commerce: Quantum Key Distribution (QKD) generates secure keys between Alice and Bob over a quantum channel. These keys are then used to encrypt data for secure transactions in telecom-based e-commerce platforms.

a higher secure key rate since fewer bits have to be discarded during privacy amplification, allowing more key material to be retained.

In practical telecom implementations, classical communication enables error correction, reconciling discrepancies between Alice's and Bob's sequences. This step may use classical error-correcting codes, such as LDPC codes, which modify the length of the raw key by discarding bits affected by errors. Finally, privacy amplification uses hash functions to compress the reconciled key, eliminating any partial information that might have been obtained by a potential eavesdropper. This filtered key is then ready for secure data encryption over telecom networks, ensuring that all information remains concealed, even if part of the initial transmission was compromised.

The efficiency in telecommunication QKD is based on the emission rate of the photon source, the transmission characteristics of the quantum channel, and the detection sensitivity of Bob's measurement devices. In this regard, "raw key rate" can be included. Dark counts are spurious clicks not related to the actual photon transmission at the detector; they contribute positively to QBER and thus are undesirable. For increasing Alice-Bob separation, transmission losses in the optical fibre or free-space link reduce the number of detectable photons, and hence reduce R_{raw}. In any practical application of QKD in commerce, dark count minimization and optimization of detector efficiency will be required to attain a feasible key rate (H.-L. Huang et al., 2017; Kirsch & Chow, 2015).

Recent developments of QKD protocols have targeted enhancing feasibility of secure key-exchange over larger distances. A general strategy here is the decoy state approach, itself developed to counter PNS attacks. In a PNS attack, an eavesdropper makes use of multi-photon signals in order to obtain information without introducing detectable anomalies. Decoy state approaches involve having Alice randomly change the intensity of the photon source such that an attacker cannot distinguish whether a single-photon or multi-photon pulse has been sent (Marshall et al., 2016). The scheme therefore enables better estimation of single-photon events produced by Alice and Bob, which are essential for secure key extraction.

There is similarly a need for adaptations toward telecom applications of QKD, considering the environmental variables such as phase stability in interferometric protocols and signal attenuation in fiber optics over long distances. Another critical area of development is quantum repeaters, enabling the extension of entanglement distances by creating intermediate nodes preserving quantum information (Mavroeidis et al., 2018).

Therefore, shifting to postquantum cryptography takes into consideration the case of telecommunication commerce with regard to vulnerabilities that quantum computing has brought upon various classical methods of encryption. Algorithms like Shor's algorithm have factorized large integers in $O((\log N)^3)$ time and have thus threatened the very security of classic cryptographic protocols such as RSA (Mavroeidis et al., 2018; Sharma et al., 2021). Therefore, lattice-based cryptography schemes emerge as a robust alternative wherein the Learning With Errors problem is at the forefront.

The LWE problem is defined by the challenge of recovering a secret vector $\mathbf{s}$ from pairs $(\mathbf{A}, \mathbf{A}s + \mathbf{e})$, where $\mathbf{A}$ is a known matrix and $\mathbf{s}$ represents the secret vector and $\mathbf{e}$ is some error vector, drawn from a discrete Gaussian distribution, that introduces noise so as to eliminate the linear relationship

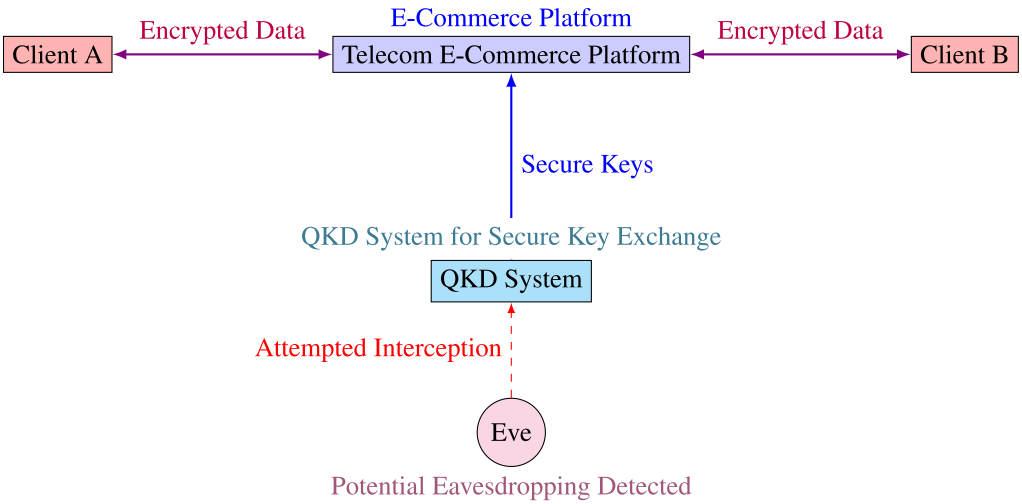

FIGURE 2. Data Flow in Secure Telecom E-Commerce: Secure keys from the QKD system are used for encrypting data transmissions between the telecom e-commerce platform and clients, ensuring confidentiality and security even in the presence of potential eavesdroppers.

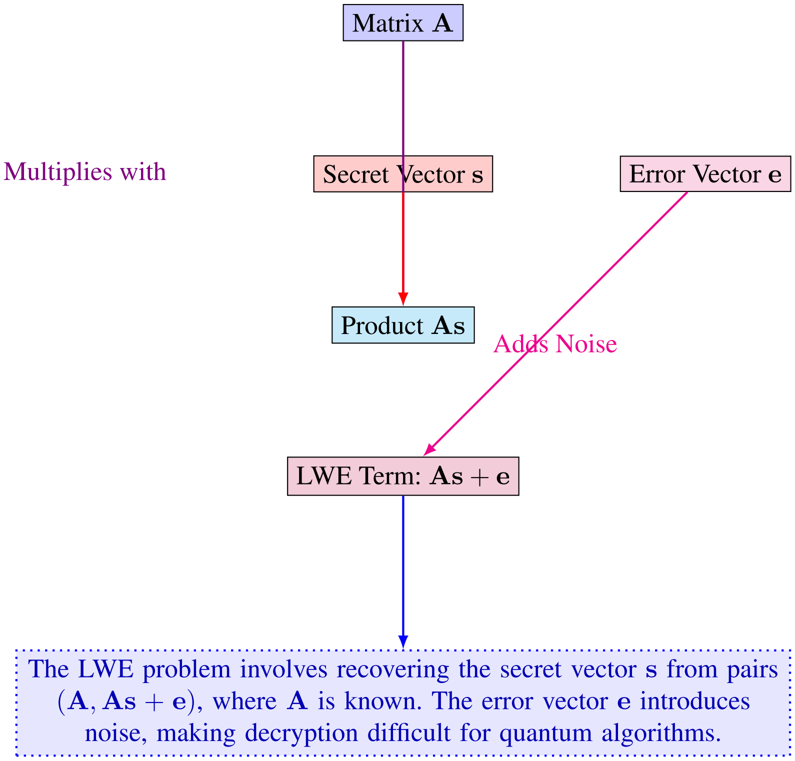
Matrix $\mathbf{A}$
Multiplies with
Secret Vector $\mathbf{s}$
Error Vector $\mathbf{e}$
Product $\mathbf{As}$
Adds Noise
LWE Term: $\mathbf{As} + \mathbf{e}$
The LWE problem involves recovering the secret vector $\mathbf{s}$ from pairs $(\mathbf{A}, \mathbf{As} + \mathbf{e})$, where $\mathbf{A}$ is known. The error vector $\mathbf{e}$ introduces noise, making decryption difficult for quantum algorithms.

FIGURE 3. LWE Problem: The hardness of computing the secret vector $\mathbf{s}$ from the noisy term $\mathbf{As} + \mathbf{e}$ is the foundational issue enabling the construction of quantum-resistant cryptographic schemes.

between $\mathbf{A}$ and $\mathbf{s}$. The resilience provided by such a nature of LWE makes it highly resistant to quantum attacks because the noise avoids direct decryption via quantum algorithms.

Telecommunication networks, which work on large-scale infrastructure, are all dependent on secure encryption of data. Usage of LWE-based encryption gives surety that in the case of an interception of stre]ams of data, the underlying information shall be secure. For example, encrypted communications between telecom servers, such as those that deal with customer billing or mobile network authentication, rely on the intractability of the problems based on LWE. Because of the error term, any attempts to decode these encrypted transmissions without access to the secret key will remain computationally infeasible, even for a quantum computer (Preskill, 2018; Zeuner et al., 2021).

The deployment of lattice-based encryption reaches to those very scenarios that include secure messaging, encrypted voice calls, and protection of financial transactions over mobile networks. In these scenarios, the LWE problem provides the basis for key-exchange protocols that make sure session keys shared between devices remain confidential. Mathematical hardness of LWE ensures that even with advances in quantum computing, the keys cannot be derived by unauthorized parties. This goes hand in hand in maintaining secure communication links across distributed telecom networks.

Ring-LWE is one of the variants of the standard LWE problem, further extending the applicability toward telecom by reducing computational complexity through the use of structured number rings instead of general matrices. Because of this reduction, it allows faster operations and efficient key management; therefore, it can also be applied to real-time encryption in high-speed communication systems. Ring-LWE can securely exchange data across network nodes by ensuring that encrypted information is totally protected throughout the transmission path from base stations to end-user devices.

That means the natural resistance of LWE to quantum decryption agrees with the requirements of 5G and 6G networks, where communication over a vast number of interconnected devices is in focus. Thus, LWE-based cryptography provides such a method for securing communications against a possible attack by a quantum-enabled eavesdropper while the scope and complexity of telecommunication networks continue to expand. The adaptation will ensure that encrypted channels are robust in everything, from cloud-based telecom services to secure mobile payments to verification of data integrity among carriers. Emphasis on lattice-based cryptography, such as LWE and its variants, provides the essential basis upon which secure telecommunication services will be maintained once quantum computing becomes viable. It ensures that user data privacy, network communication integrity, and encrypted information confidentiality remain intact, irrespective of developments in computational power.

IV. QUANTUM ALGORITHMS FOR SPEED OPTIMIZATION

In the context of telecom e-commerce, QAOA is an especially powerful method of combinatorial optimization problems that involve the optimization of network operations and resource management. QAOA is a variational algorithm in which quantum mechanics iteratively refines parameters toward near-optimal solutions in complex optimization problems (Bub, 2010). This will be done by implementing a series of parameterized unitary transformations on an initial quantum state:

$$|\psi(\boldsymbol{\gamma},\boldsymbol{\beta})\rangle = U(B,\beta_p)U(C,\gamma_p)\cdots U(B,\beta_1)U(C,\gamma_1)|\psi_0\rangle.$$

Here, the unitary transformations $U(B,\beta) = e^{-i\beta B}$ and $U(C,\gamma) = e^{-i\gamma C}$ define the evolution of the quantum state. The operators B and C correspond to the problem constraints and the objective function, respectively. The parameters $\boldsymbol{\gamma} = (\gamma_1,\gamma_2,\ldots,\gamma_p)$ and $\boldsymbol{\beta} = (\beta_1,\beta_2,\ldots,\beta_p)$ are adjusted iteratively to improve the solution quality.

Most of the typical optimization problems of telecom e-commerce usually deal with such tasks as routing network traffic, which is to be efficiently directed through a network in order to minimize latency or congestion. Likewise, resource allocation problems come up when bandwidth or server capacity has to be divided among several users or services in a way that optimizes throughput and cuts costs. QAOA does indeed provide a scheme where, for example, telecom operators can translate such problems into a cost function C, which characterizes efficiency of the network or sum of resource utilization to be minimized or maximized (Buchanan & Woodward, 2017; Farhi et al., 1998). In this, the algorithm attempts to maximize the expectation value of the cost function within the state prepared by the parameterized quantum circuit:

$$\langle\psi(\boldsymbol{\gamma},\boldsymbol{\beta})|C|\psi(\boldsymbol{\gamma},\boldsymbol{\beta})\rangle.$$

This expectation value tells us how far the current parameter settings $\boldsymbol{\gamma}$ and $\boldsymbol{\beta}$ are from the optimal solution. Iteratively adjusting the parameters using a classical optimizer yields, in the limit, a quantum state that corresponds to an approximate solution of the problem under study. Thus QAOA is a hybrid quantum-classical algorithm appropriate for today's generation of Noisy Intermediate-Scale Quantum devices, based on shallow quantum circuits with a modest number of qubits.

QAOA can give a competitive advantage in telecom e-commerce, as poor resource management here directly influences the user experience and operational costs. In any case where there is the need for the dynamic allocation of bandwidth to different regions from a telecom provider, one that requires matching fluctuating demands, QAOA can find an optimal way to strategize bandwidth allocation for maximum network efficiency while minimizing congestion. This is accomplished by encoding the topology and traffic into the problem Hamiltonian C and iteratively refining the quantum

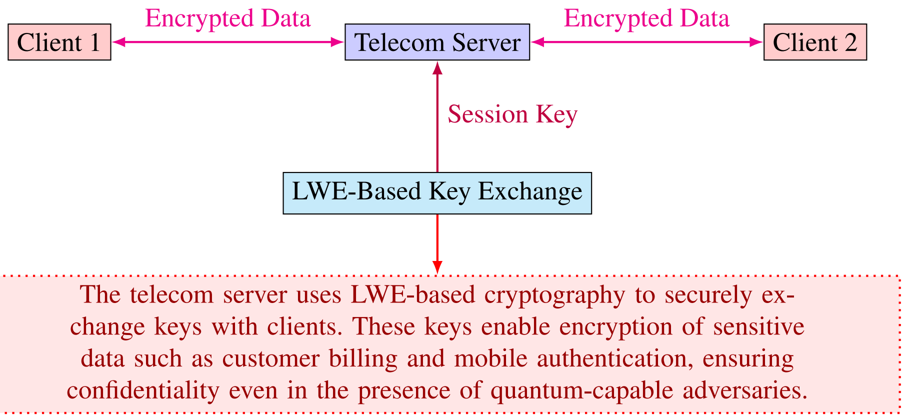
Client 1
Encrypted Data
Telecom Server
Encrypted Data
Client 2
Session Key
LWE-Based Key Exchange
The telecom server uses LWE-based cryptography to securely exchange keys with clients. These keys enable encryption of sensitive data such as customer billing and mobile authentication, ensuring confidentiality even in the presence of quantum-capable adversaries.

FIGURE 4. Lattice-Based Cryptography Applied in Telecom E-Commerce: The key exchange based on LWE will ensure that encrypted data is sent securely between the telecom servers and clients, hence keeping the communication safe from quantum-based attacks.

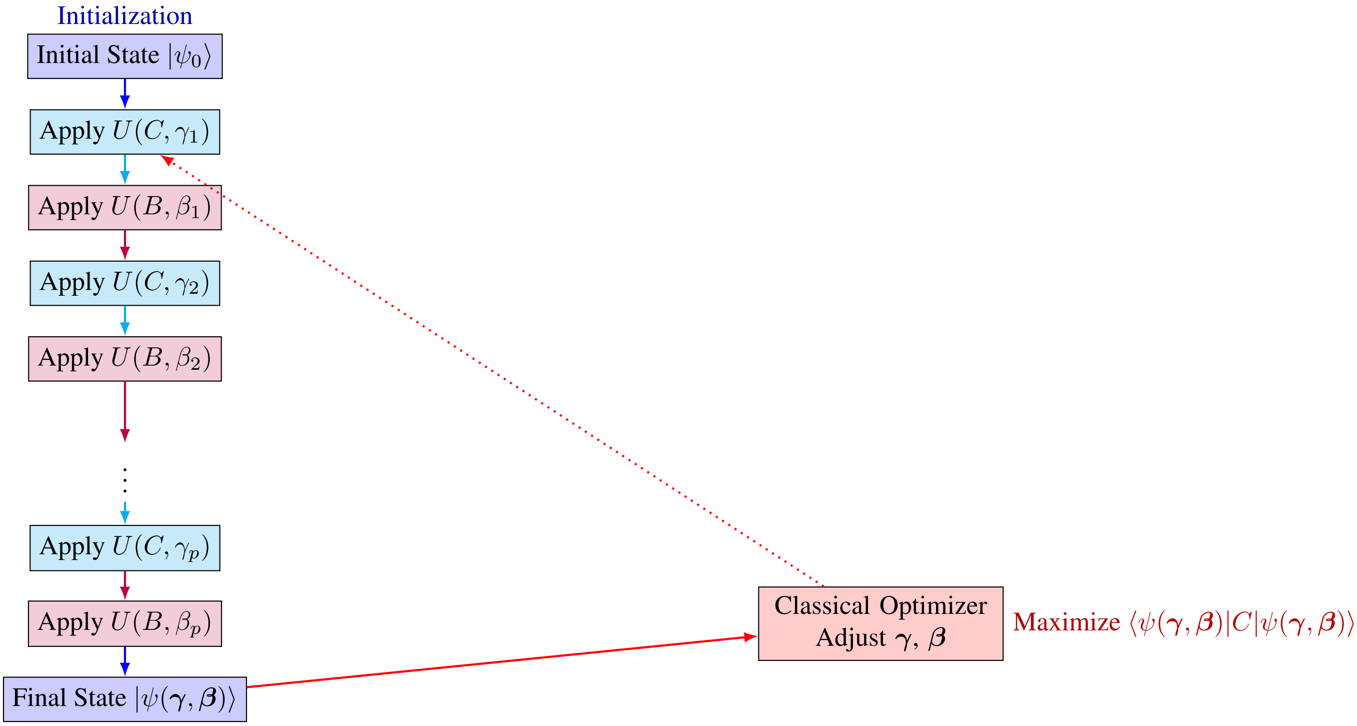
Initialization
Initial State $|\psi_0\rangle$
Apply $U(C,\gamma_1)$
Apply $U(B,\beta_1)$
Apply $U(C,\gamma_2)$
Apply $U(B,\beta_2)$
Apply $U(C,\gamma_p)$
Apply $U(B,\beta_p)$
Final State $|\psi(\boldsymbol{\gamma},\boldsymbol{\beta})\rangle$
Classical Optimizer
Adjust $\boldsymbol{\gamma}$, $\boldsymbol{\beta}$
Maximize $\langle\psi(\boldsymbol{\gamma},\boldsymbol{\beta})|C|\psi(\boldsymbol{\gamma},\boldsymbol{\beta})\rangle$

FIGURE 5. QAOA Process: The algorithm iteratively applies parameterized unitary transformations $U(C,\gamma)$ and $U(B,\beta)$ to go an initial state $|\psi_0\rangle$ toward a near-optimal solution. A classical optimizer adjusts the parameters γ and β based on the expectation value of the cost function.

state to minimize the costs associated with either suboptimal routing or over-allocated resources (Jozsa & Linden, 2003).

Also, QAOA might be applied against the scheduling workloads of data centers operating e-commerce transactions to optimize server workloads and lower power consumption. QAOA can find configurations that minimize latency for users accessing online services by modeling the task scheduling problem as a combinatorial optimization problem; this would help improve the responsiveness and reliability of e-commerce platforms. This includes the optimization of parameters with the use of classical algorithms, such as gradient-based methods or gradient-free optimizers, by iteratively updating γ and β until the expectation value of the solution is maximized.

It is in the application of QAOA to these telecom-specific problems that one finds the grounds for directly tapping into computational strengths that quantum algorithms will provide. In turn, this enables the investigation of exponentially large solution spaces, inaccessible to classical algorithms in reasonable time, and may be key to faster convergence to near-optimal solutions in complex scenarios where traditional methods may struggle. Hence, QAOA can be applied for the effective development of operational methods of telecom e-commerce providers by improving service delivery and optimizing the use of network resources (Prevedel et al., 2007).

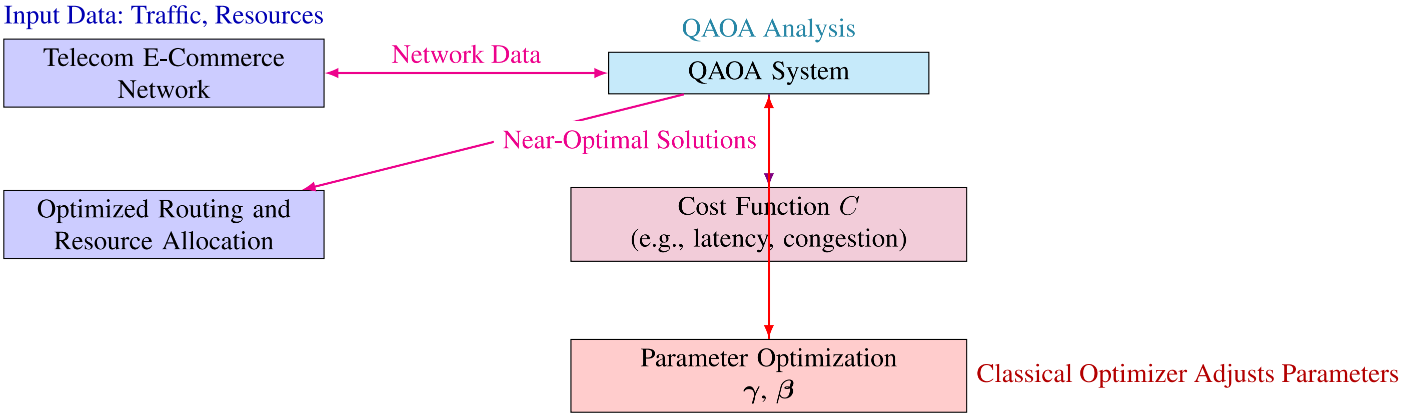
Input Data: Traffic, Resources
Telecom E-Commerce Network
Network Data
QAOA Analysis
QAOA System
Near-Optimal Solutions
Optimized Routing and Resource Allocation
Cost Function C (e.g., latency, congestion)
Parameter Optimization γ, β
Classical Optimizer Adjusts Parameters

FIGURE 6. QAOA Application in Telecom E-commerce: QAOA is put into telecom network operations optimisation, like traffic routing or resource allocation, by formulating these problems into a cost function C. This algorithm iteratively adjusts parameters γ and β to find near-optimal solutions that enhance network efficiency.

It provides a quadratic speedup in unstructured search problems and Grover's search algorithm has pragmatic applications in telecom e-commerce in all situations involving large databases and their associated need for rapid access to data. In searching for an element in a database of size N, Grover's algorithm can find the marked item among those in $O(\sqrt{N})$ time, a considerable improvement compared with classical search algorithms, that would require $O(N)$ time to linearly search through the entire database.

The area where the efficiency of data processing directly touches the quality of the service by the customer is telecommunications in e-commerce. Grover's algorithm may be put to work to improve the speed of searches through the large databases of queries from users. For example, when the processing of a customer query is involved, or fetching user account information from a large database, the speedup afforded by Grover's algorithm reduces latency and enables the telecoms provider to give faster responses to user requests (Gupta & Nene, 2020). This can be particularly useful during peak loads, wherein effective fetching of data enhances the experience for the user and ensures that the e-commerce sites are responsive.

Going beyond mere retrieval, Grover's algorithm finds applications in more complex tasks, such as fraud detection. The usual telecom e-commerce systems usually have to find out the anomalies in transactions or patterns depicting fraud transactions amidst the large volume of transactions. In this manner, by reducing the search problem of specific fraud patterns, Grover's algorithm can rapidly sift through the records in search of entries that may be suspicious. This, in fact, enables near-real-time fraud detection, since such a quadratic reduction in search time leads to quicker responses and mitigations for maintaining the integrity of financial transactions and customer trust (Stock & James, 2009).

Grover's algorithm works by iteratively applying a set of quantum operations, called the Grover iteration, that systematically increase the probability amplitude of the target state, often referred to as the "marked" item, while dampening that of all the other states. This is done via the iteration expressed by the Grover diffusion operator:

$$G = 2|\psi\rangle\langle\psi| - I,$$

where G is applied in succession onto the quantum state $|\psi\rangle$ that represents the equal superposition of all possible entries in the database. After roughly $\sqrt{N}$ steps the algorithm shifts the probability distribution so that upon measurement of the quantum state it will return the marked item with high probability (Rawat et al., 2022).

That is to say, in certain telecom e-commerce applications, the search for some specific user records or patterns in transaction data is bound to be much faster compared to classical search algorithms. For example, Grover's algorithm can speed up the analysis while a telecom provider goes through call records or purchase histories in order to find out the pattern of user behavior or to segment customers. This will be useful for real-time applications, where the ability for fast access to user information allows for personalization, better targeting of marketing efforts, or immediate verification during customer support calls (Riel, 2021).

Besides, Grover's algorithm may be applied in enhancing backend procedures; for example, database maintenance and optimization, wherein some search for a data structure or record is to be singled out from a dataset. Grover's algorithm provides quadratic speed-up in such processes, and this management of computational resources is much easier and saves time in data processing. Though this fact contributes to operational efficiency for the e-commerce platforms, reducing latency is important in a competitive market environment wherein user satisfaction directly influences retention and revenue.

V. AI-DRIVEN CUSTOMER EXPERIENCE USING QUANTUM MACHINE LEARNING (QML)

Quantum Support Vector Machines embed classical data into high-dimensional quantum state spaces and incorporate elements of quantum computing into conventional SVMs.

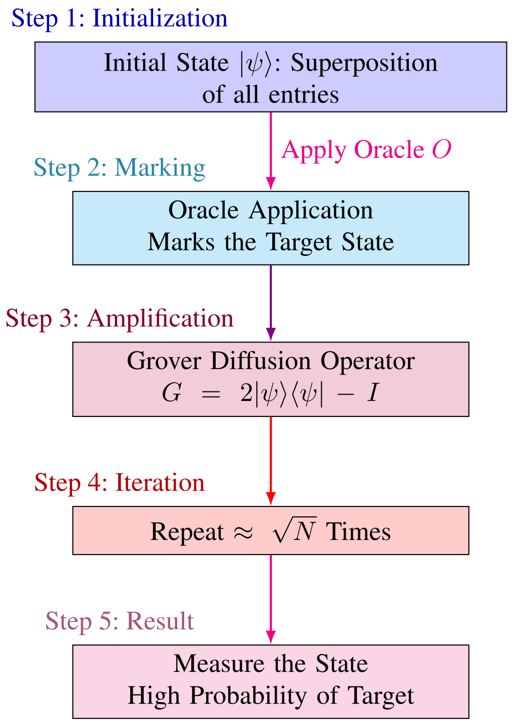
Step 1: Initialization
Initial State $|\psi\rangle$: Superposition of all entries
Apply Oracle O
Step 2: Marking
Oracle Application Marks the Target State
Step 3: Amplification
Grover Diffusion Operator $G = 2|\psi\rangle\langle\psi| - I$
Step 4: Iteration
Repeat $\approx \sqrt{N}$ Times
Step 5: Result
Measure the State High Probability of Target

FIGURE 7. Grover's search algorithm starts with an initial superposition state where the oracle applied marks the target state, followed by the Grover diffusion operator that amplifies the probability of the target. For about $\sqrt{N}$ iterations later, the target state can be measured with high probability.

The process begins with the training data in classical form G that is given as $(\mathbf{x}_i, y_i)$, where $\mathbf{x}_i$ is the feature vector, while $y_i \in \{-1, 1\}$ are class labels. Quantum feature maps are used to embed each input vector $\mathbf{x}_i$ into a quantum state $\phi(\mathbf{x}_i)$, projecting the data into a complex quantum space. The basic construction of QSVM is based on the quantum kernel $K(\mathbf{x}, \mathbf{x}')$ defined by $|\langle\phi(\mathbf{x})|\phi(\mathbf{x}')\rangle|^2$. This kernel captures the similarity between two quantum states, thus making it possible to realize much finer similarity calculations compared to classical kernels (Abohashima et al., 2020; Chen & Yoo, 2021).

The most basic advantage of QSVM concerns its capability to implicitly calculate the similarity measure in high-dimensional spaces by means of quantum state representations. In the case of classical SVM, at least for cases where one has to deal with complicated datasets, computation of the feature maps has to be performed explicitly. This very rapidly becomes computationally prohibitive with growing dimensionality. In contrast, QSVM uses quantum states to carry out such mappings implicitly, thus enabling the efficient calculation of inner products between quantum-encoded data points. This approach is beneficial in datasets containing large numbers of features, such that the exponential nature of quantum space can represent intricate structures that would be challenging for classical methods to process (Schatzki et al., 2021; Suzuki & Katouda, 2020).

In QSVM, one common method for encoding classical data into quantum states is called amplitude encoding. It works by mapping the features of data into the amplitude probabilities of quantum states. Using this technique, an exponential number of features can be encoded into a logarithmic number of qubits. For instance, n features can be encoded into $\log(n)$ qubits, thereby compressing the feature space. This encoding is necessary to minimize resources that need to be spent during quantum processing, since large amounts of data can be dealt with using this method in the constraints of present quantum hardware. Representing data in this form, the quantum kernel $K(\mathbf{x}, \mathbf{x}')$ provides the measure of overlap between the amplitude-encoded states computable through suitably designed quantum circuits (Duan et al., 2020).

The methods used in the QSVM are hybrid, integrating quantum and classical methodologies. While the quantum processor is responsible for the computation of the kernel function, in general, the parameters of the SVM model are classically optimized during the training process. The hybrid approach is usually carried out with the help of a VQA in which the decision boundary is optimized in an iterative manner from feedback provided by classical optimization loops, which are guided by quantum-encoded similarities. This training form essentially provides the advantage of quantum processing without essentially needing a fully quantum system; hence, this is suitable for handling high-dimensional data streams typical in telecom e-commerce (Duan et al., 2020; Dunjko & Wittek, 2020).

QSVMs can efficiently classify and analyze high-dimensional and diverse datasets that contain customer purchase behavior, service usage patterns, and real-time inter-

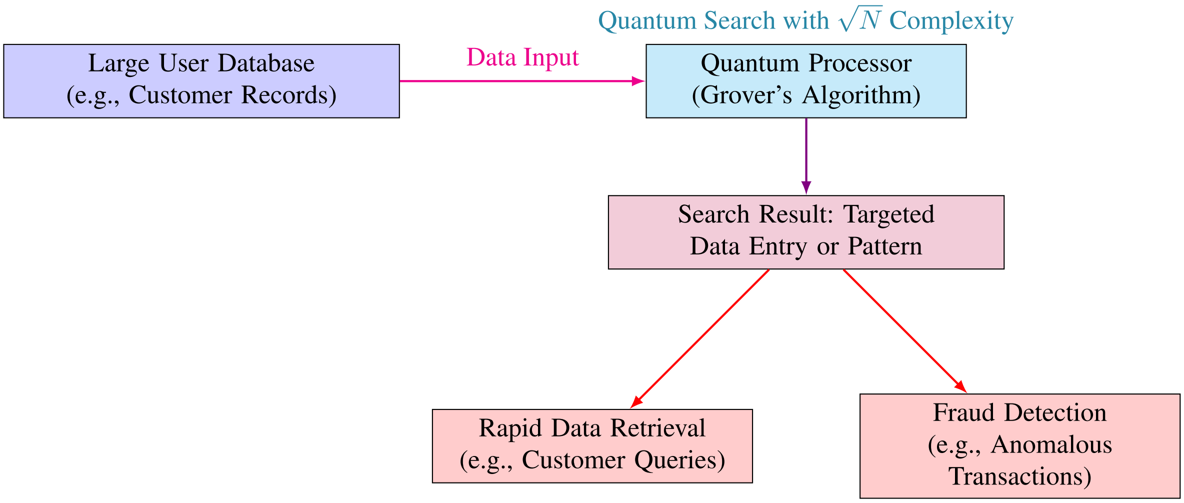
Quantum Search with $\sqrt{N}$ Complexity
Large User Database (e.g., Customer Records)
Data Input
Quantum Processor (Grover's Algorithm)
Search Result: Targeted Data Entry or Pattern
Rapid Data Retrieval (e.g., Customer Queries)
Fraud Detection (e.g., Anomalous Transactions)

FIGURE 8. Application of Grover's Algorithm in Telecom E-Commerce: The quantum processor utilizes Grover's algorithm to search through large databases, providing speed-ups in data retrieval tasks such as processing customer queries or detecting fraud. The quadratic reduction in search time enables faster and more efficient data analysis.

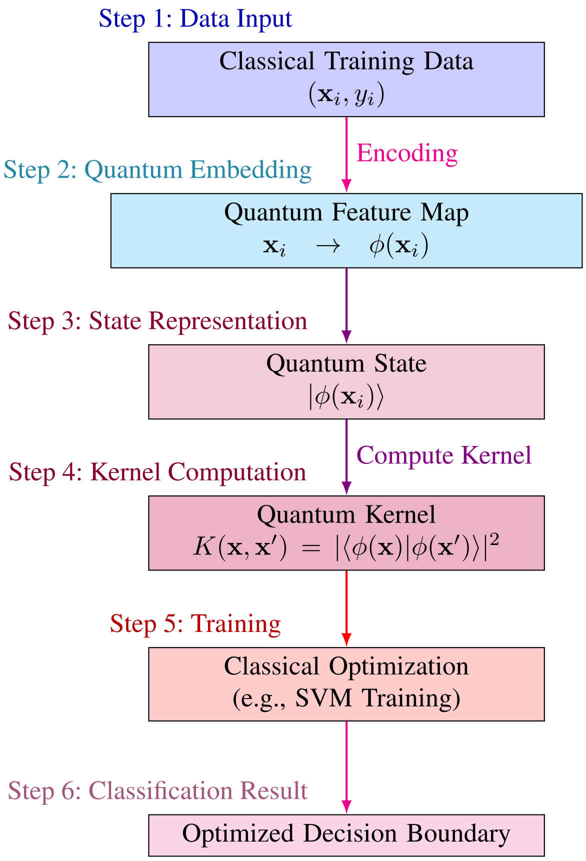
Step 1: Data Input
Classical Training Data $(\mathbf{x}_i, y_i)$
Encoding
Step 2: Quantum Embedding
Quantum Feature Map $\mathbf{x}_i \rightarrow \phi(\mathbf{x}_i)$
Step 3: State Representation
Quantum State $|\phi(\mathbf{x}_i)\rangle$
Compute Kernel
Step 4: Kernel Computation
Quantum Kernel $K(\mathbf{x}, \mathbf{x}') = |\langle\phi(\mathbf{x})|\phi(\mathbf{x}')\rangle|^2$
Step 5: Training
Classical Optimization (e.g., SVM Training)
Step 6: Classification Result
Optimized Decision Boundary

FIGURE 9. QSVM Process: Classical data is embedded into quantum states using quantum feature maps, allowing for the computation of a quantum kernel. The kernel is used in a classical optimization loop to train the SVM, yielding a decision boundary based on quantum-encoded similarities.

action data in telecom e-commerce. In the practical case of customer churn prediction, QSVMs employ the quantum kernel to project the pattern of customer behaviors onto the quantum state space and enable the identification of a separating hyperplane that distinguishes between churning and loyal customers. The quantum approach enables the consideration of a huge number of features together; classical models will be too slow or cannot track some pattern or relationship. QSVM enables the refinement of predictive models for more precise retention strategies and a better understanding of customer life cycle patterns by leveraging high-dimensionality quantum space (B. Huang et al., 2020; Khan & Robles-Kelly, 2020).

Moreover, QSVMs are able to process the complicated relationships of words in sentiment analysis, much needed when interpreting customer feedback and engagement data in telecom e-commerce. Thus, the ability of quantum kernels to represent text features in high-dimensional space empowers QSVMs to capture subtle differences in context and sentiment, moving beyond superficial meaning representation, which is inherent in classical methods. In contrast to the classical models, which often rely on hand-designed feature maps or pre-trained embeddings, QSVMs would inherently encode such complex relationships through quantum feature mappings, hence increasing the accuracy of sentiment classification (Quiroga et al., 2021). The encoded data shall construct decision boundaries that realistically reflect the subtlety of customer feedback and therefore improve insights from customer interactions.

Various deployments of QSVMs in these domains hint at the potential of quantum computing for enhancing machine learning tasks due to basic principles of quantum mechanics. QSVMs will provide a sound framework for classification tasks where large and complex data need to be handled by representation in quantum states and quantum kernel calculation. The transformation of the classical input data into the quantum state space does not only allow for much more efficient computation of similarities but also makes visible certain intricate patterns that could be invisible to classic SVMs. The QSVM model therefore represents an important evolution in the use of support vector machines by means of quantum mechanics for predictive analytics in data-intensive industries like telecom e-commerce (Sheng & Zhou, 2017; Zaspel et al., 2018).

VI. DECOHERENCE AND GATE ERRORS

This sensitivity to noise, resulting from decoherence and gate errors, is among the major challenges quantum systems have to confront. These make the loss of quantum information difficult, hence reliable computation as well. Quantum error correction overcomes this problem by way of use of entangled qubits for error detection and correction without direct measurement of the quantum state, which keeps the fragile superpositions intact.

Among the most well-known QEC schemes is the surface code, in which qubits are placed in a two-dimensional lattice structure such that neighboring qubits are entangled. Such structuring of qubits can find single bit-flip and phase-flip errors because of its ability to measure the stabilizer operators-quantum parity checks finding inconsistencies introduced by the errors. The logical qudit of the surface code comprises a large number of physical qubits with the purpose of providing redundancy for the correction of errors detected in them.

The code distance d defines the error-correcting capability of a given QEC code:

$$d = 2t + 1,$$

where t would be the maximum number of errors that it is possible to correct. The larger the code distance, the more errors the system can tolerate-but the number of physical qubits needed to encode a single logical qubit grows correspondingly. One can easily show that correcting one error requires a code distance of 3. While increasing d does increase the coherence time over which the quantum processor can perform accurate computations, this is clearly at the expense of greater resource requirements.

This is to say that fault tolerance, when quantum gate error rates are below a certain threshold that can be managed with QEC codes, stands out as an important capability for scalable quantum computing. In telecom e-commerce, this capability is high because it allows for proper and undisturbed execution of quantum algorithms underlying tasks, such as secure communication protocols, optimized resource management, and advanced data analysis. Fault-tolerant quantum processors are those that ensure these computations are done in an accurate manner even when physical imperfections abound in the hardware of quantum systems.

Among various leading candidates that implement fault tolerance in quantum processors, the surface code stands tall because of its high error tolerance. However, one of the major challenges to scaling up quantum systems is the very resource-intensive nature of QEC, where hundreds to thousands of physical qubits are used to keep a single logical qubit. While quantum hardware is bound to evolve, the dire need is for developing efficient QEC methods; only that way could quantum computing possibilities be harnessed by the telecom e-commerce platforms without deterioration due to the influence of noise and errors.

Quantum computing in telecom applications also brings challenges in terms of interfacing with classical systems and managing the data transfer rates between QPUs and classical processors. Systems take advantage of the strength of each processor type: QPUs execute tasks best suited for quantum algorithms, while the classical processor handles routine computations and control operations. Seamless communication may be at the heart of integration effectiveness. First, there is a gap in data rate and processing speed from quantum to classical. Whereas the classical processors could work with very high rates of data processing, QPUs can only have much slower cycles of operation, especially considering the generation of NISQ now, which requires precise manip-

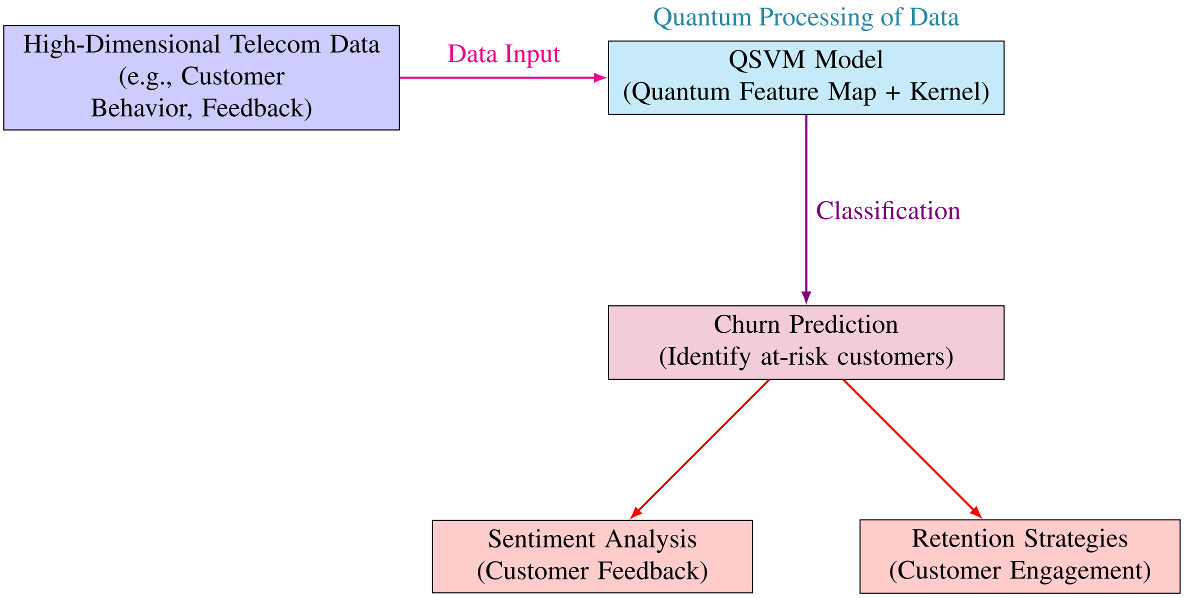
High-Dimensional Telecom Data (e.g., Customer Behavior, Feedback)
Data Input
Quantum Processing of Data
QSVM Model (Quantum Feature Map + Kernel)
Classification
Churn Prediction (Identify at-risk customers)
Sentiment Analysis (Customer Feedback)
Retention Strategies (Customer Engagement)

FIGURE 10. QSVM Usage in Telecom E-commerce: QSVM finds its application in telecom data classification, which involves high-dimensional data. For example, telecom patterns related to customer behavior or its feedback. The insights from classification based on quantum help predict churn, perform sentiment analysis, and develop retention strategies accordingly.

TABLE 3. Comparison of Quantum Error Correction Codes

QEC Code	Code Distance (d)	Correctable Errors (t)	Physical Qubits per Logical Qubit
Surface Code	$d = 3, 5, 7, \ldots$	$t = \frac{d-1}{2}$	$O(d^2)$
Steane Code	$d = 3$	$t = 1$	7
Shor Code	$d = 3$	$t = 1$	9
Bacon-Shor Code	$d = 3, 5$	$t = \frac{d-1}{2}$	$O(d^2)$
[[7,1,3]] Code	$d = 3$	$t = 1$	7

TABLE 4. Resource Requirements for Surface Code Implementation

Code Distance (d)	Number of Correctable Errors (t)	Approximate Physical Qubits per Logical Qubit
3	1	~ 13
5	2	~ 25
7	3	~ 49
9	4	~ 81
11	5	~ 121
15	7	~ 225
21	10	~ 441

TABLE 5. Comparison of Quantum and Classical Processor Characteristics

Characteristic	Quantum Processing Unit (QPU)	Classical Processor
Data Processing Speed	Slower (due to qubit manipulation)	Faster (GHz-range clock speeds)
Data Rate	Lower (NISQ era constraints)	Higher (suitable for high-throughput tasks)
Error Rates	Higher (requires Quantum Error Correction)	Lower (mature error-handling methods)
Application Focus	Optimization, cryptography, quantum simulations	Control tasks, real-time processing, routine calculations
Integration Role	Provides solutions for complex problems	Manages control, interfaces, and overall workflow

ulations over qubit states with implemented error mitigation. This mismatch creates the need for interfaces that have to be designed with care such that data transfer does not become the bottleneck. An efficient interfacing of quantum-classical means translation of the quantum results into formats that can easily be either processed or acted upon by classical systems quickly and with minimal latency in an end-to-end workflow.

With the same hybrid systems in telecommunication e-commerce, any number of applications can be included: quantum algorithms for optimization of network routing, while a classical system performs real-time monitoring and adjusts the traffic. In this case, the quantum part will process some complex problems of optimization and return results to the classical system for implementation in the network infrastructure. The integration layers of such an approach need to efficiently manage the translation of quantum outputs into actionable data, so that the results can be used in near real-time applications.

Effective interfacing of QPUs with classical processors requires strong protocols for data transmission that can bear the peculiar demands associated with quantum data, such as coherence in cases where the quantum information needs coherence. This may be achieved by employing high-bandwidth channels of communication or using low-latency protocols for data transfer so as to avoid latencies or losses that could render communication between the classical and quantum parts nullified.

Second, control systems play an important role in managing the hybrid environment, determining when to invoke quantum computation and how to incorporate the outputs into broader processes managed by classical systems. Notably, this coordination is an important part of practical implementations in telecom networks where decisions based on quantum computations, such as dynamic bandwidth allocation or secure cryptographic key management, are supposed to be integrated seamlessly into existing classical workflows.

VII. CONCLUSION

Quantum computing revisits the ways of approaching computationally demanding problems by including unique properties of qubits and their interaction with quantum mechanics. Qubits can exist in superposition states; that is, they hold many values at a time while enabling parallelism in computation. Entanglement, one of the basic principles that underlines this aspect, establishes non-local correlation between qubits, enabling their states to influence each other over large distances. These phenomena enable quantum systems to solve problems containing extensive parallel processing, hence being effective in tasks that are computationally infeasible for classical methods. An example is that, while difficult for classical algorithms, integer factorization could be addressed more efficiently with quantum algorithms, achieving polynomial time complexity where the classical methods would require exponential time. This, in turn, has a profound impact on cryptographic systems, as in most encryption schemes, their security relies precisely on the computational hardness of tasks like factorization. The advent of quantum algorithms casts doubt on the resilience of classical cryptography against eventual quantum attacks.

Quantum Key Distribution, QKD, represents one such way to perform secure communication with its security relying on the intrinsic properties of quantum mechanics in key exchange processes. Contrary to classical cryptographic, where the tapping may not be detected, QKD relies on a fundamental quantum mechanical principle: measurement perturbs a quantum state. For example, in the BB84 protocol, Alice sends qubits encoded in random bases to Bob, who measures them in randomly chosen bases. A process of comparing subsets of these measurements reveals any disturbances introduced by an eavesdropper, as interception would alter the states of the qubits. An error rate measured, the Quantum Bit Error Rate, or QBER, gives itself a measure of the presence of probable interception. High QBER would therefore mean higher chances of eavesdropping, in which case Alice and Bob would discard the compromised key. This is the mechanism that ensures QKD provides security against any kind of potential threat from quantum computers, which may decrypt classically encrypted data.

Besides cryptography, quantum computing applies in solving complex optimization problems arising in areas such as telecommunications. Resource allocation, traffic management, and latency minimization are challenges within one big category that is very often characterized by large and complex search spaces. For large and complex search spaces, classical methods of optimization become inefficient. It applies to this through the use of quantum states in the more efficient investigation of the solution space. QAOA starts with some initial quantum state and transforms this in a stepwise manner via unitary transformations, specified via parameters, which are iteratively updated in a way that converges to an optimal solution. The cost and mixer Hamiltonians are applied to influence the evolution of the quantum state during QAOA. These guide the exploration of the solution space to refine its search for the best outcome. It is for this reason that QAOA can come out with a solution in a number of iterations compared with classical algorithms, thereby saving computational time for tasks such as routing traffic and bandwidth management in telecom networks.

Quantum machine learning is another important domain in which quantum computing opens new perspectives for enhancing computational models with complex data analysis. Most of the applications have to operate with high-dimensional data, such as customer behavior and predictive analytics in telecom e-commerce. Conventional algorithms in machine learning often face computational problems when dealing with this type of data because the feature space increases exponentially. Such problems are resolved by quantum-enhanced models such as QSVM and quantum neural networks, which map input data to high-dimensional quantum state spaces for speedier processing and convergence. For instance, the QSVM makes use of a quantum kernel that evaluates inner products between quantum-encoded

TABLE 6. Key Considerations in Quantum-Classical Integration for Telecom Applications

Aspect	Challenges	Solutions
Data Rate Mismatch	Slow quantum cycles vs. fast classical processing	High-bandwidth channels, buffering
Latency	Delays in translating quantum results	Optimized protocols, parallel classical tasks
Quantum Errors	Noisy results from inherent error rates	QEC codes, error mitigation techniques
Data Transmission	Coherence maintenance during transfer	Low-latency protocols, error-corrected lines
Control Coordination	Synchronization of quantum and classical tasks	Adaptive control, dynamic allocation
Real-Time Integration	Delays for real-time applications	Hybrid algorithms, pre-processing, feedback loops

data points to enable such separations of complex patterns that are difficult or practically infeasible for a classical model to resolve. With QML models promising a more effective method of calculating decision boundaries in high-dimensional feature spaces, they could hopefully enhance classification tasks and predictive analytics in e-commerce and change how customer interactions should be analyzed and optimized.

Quantum computing still faces significant challenges in the road to actual implementation for practical uses, concerned with hardware stability and integration into classical systems. Qubit decoherence is among the major issues: because of interactions with the environment, the quantum state of a qubit collapses into one of its basis states, and such information is lost. Coherence time determines how long a qubit can really keep its quantum state and depends on external noise and thermal interactions. Most notably, long coherence times are a prerequisite for effective quantum computation, and this usually requires sophisticated techniques such as cryogenic cooling and magnetic shielding. Quantum error correction fights the decoherence effects in their effort to preserve computational integrity, but it is bound to be costly in hardware complication. The codes correcting errors demand such encoding of a single logical qubit by multiple physical qubits that creates a huge overhead in a number of qubits required. This obviously makes the scalability of state-of-the-art quantum hardware limited, as error thresholds for fault-tolerant quantum computing require a large number of physical qubits.

In addition to this, the bottleneck due to quantum-classical integration exacerbates challenges related to data transfer and processing bottlenecks. Where classical processors are more adept at general-purpose computations, the quantum processors have particular optimizations toward specific problem types. Hybrid modes of computing, therefore, attempt to achieve this synergy by offloading certain tasks to quantum processors and the rest to classical processors. In such hybrid models, an efficient interface is required to exchange data between quantum and classical systems. It becomes of paramount importance that these interfaces operate with minimum latency, as much of the benefits accrued through quantum computation will be nullified if the transfer of data between these systems introduces too much latency. The development of lowlatency communication protocols is being studied; hybrid system architecture is being optimized in such a way that frameworks will be built to easily integrate quantum processors into existing computation workflows, particularly in telecommunication and e-commerce.

References

Abohashima, Z., Elhosen, M., Houssein, E. H., & Mohamed, W. M. (2020). Classification with quantum machine learning: A survey. *arXiv preprint arXiv:2006.12270*.

Bennett, C. H., Bernstein, E., Brassard, G., & Vazirani, U. (1997). Strengths and weaknesses of quantum computing. *SIAM journal on Computing*, *26*(5), 1510–1523.

Bova, F., Goldfarb, A., & Melko, R. G. (2021). Commercial applications of quantum computing. *EPJ quantum technology*, *8*(1), 2.

Bub, J. (2010). Quantum computation: Where does the speed-up come from. *Philosophy of quantum information and entanglement*, 231–246.

Buchanan, W., & Woodward, A. (2017). Will quantum computers be the end of public key encryption? *Journal of Cyber Security Technology*, *1*(1), 1–22.

Chen, S. Y.-C., & Yoo, S. (2021). Federated quantum machine learning. *Entropy*, *23*(4), 460.

DiVincenzo, D. P. (1995). Quantum computation. *Science*, *270*(5234), 255–261.

Duan, B., Yuan, J., Yu, C.-H., Huang, J., & Hsieh, C.-Y. (2020). A survey on hhl algorithm: From theory to application in quantum machine learning. *Physics Letters A*, *384*(24), 126595.

Dunjko, V., & Wittek, P. (2020). A non-review of quantum machine learning: Trends and explorations. *Quantum Views*, *4*, 32.

Farhi, E., Goldstone, J., Gutmann, S., & Sipser, M. (1998). Limit on the speed of quantum computation in determining parity. *Physical Review Letters*, *81*(24), 5442.

Fisher, K. A., Broadbent, A., Shalm, L., Yan, Z., Lavoie, J., Prevedel, R., Jennewein, T., & Resch, K. J. (2014). Quantum computing on encrypted data. *Nature communications*, *5*(1), 3074.

Gong, C., Du, J., Dong, Z., Guo, Z., Gani, A., Zhao, L., & Qi, H. (2020). Grover algorithm-based quantum homomorphic encryption ciphertext retrieval scheme in quantum cloud computing. *Quantum Information Processing*, *19*, 1–17.

Gruska, J., et al. (1999). *Quantum computing* (Vol. 2005). McGraw-Hill London.

Gupta, M., & Nene, M. J. (2020). Quantum computing: An entanglement measurement. *2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI)*, 1–6.

Hassija, V., Chamola, V., Saxena, V., Chanana, V., Parashari, P., Mumtaz, S., & Guizani, M. (2020). Present landscape of quantum computing. *IET Quantum Communication*, *1*(2), 42–48.

Huang, B., Symonds, N. O., & von Lilienfeld, O. A. (2020). Quantum machine learning in chemistry and materials. *Handbook of Materials Modeling: Methods: Theory and Modeling*, 1883–1909.

Huang, H.-L., Zhao, Y.-W., Li, T., Li, F.-G., Du, Y.-T., Fu, X.-Q., Zhang, S., Wang, X., & Bao, W.-S. (2017). Homomorphic encryption experiments on ibm's cloud quantum computing platform. *Frontiers of Physics*, *12*, 1–6.

Jozsa, R., & Linden, N. (2003). On the role of entanglement in quantum-computational speed-up. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, *459*(2036), 2011–2032.

Khan, T. M., & Robles-Kelly, A. (2020). Machine learning: Quantum vs classical. *IEEE Access*, *8*, 219275–219294.

Kirsch, Z., & Chow, M. (2015). Quantum computing: The risk to existing encryption methods. *Retrieved from URL: http://www. cs. tufts. edu/comp/116/archive/fall2015/zkir sch. pdf*.

Kitaev, A. Y., Shen, A., & Vyalyi, M. N. (2002). *Classical and quantum computation*. American Mathematical Soc.

Knill, E. (2005). Quantum computing with realistically noisy devices. *Nature*, *434*(7029), 39–44.

Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., & O'Brien, J. L. (2010). Quantum computers. *nature*, *464*(7285), 45–53.

Marshall, K., Jacobsen, C. S., Schäfermeier, C., Gehring, T., Weedbrook, C., & Andersen, U. L. (2016). Continuous-variable quantum computing on encrypted data. *Nature communications*, *7*(1), 13795.

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. *arXiv preprint arXiv:1804.00200*.

McMahon, D. (2008). *Quantum computing explained*. John Wiley & Sons.

Nielsen, M. A., & Chuang, I. L. (2001). *Quantum computation and quantum information* (Vol. 2). Cambridge university press Cambridge.

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information*. Cambridge university press.

O'brien, J. L. (2007). Optical quantum computing. *Science*, *318*(5856), 1567–1570.

Preskill, J. (2018). Quantum computing in the nisq era and beyond. *Quantum*, *2*, 79.

Prevedel, R., Walther, P., Tiefenbacher, F., Böhi, P., Kaltenbaek, R., Jennewein, T., & Zeilinger, A. (2007). High-speed linear optics quantum computing using active feed-forward. *Nature*, *445*(7123), 65–69.

Quiroga, D., Date, P., & Pooser, R. (2021). Discriminating quantum states with quantum machine learning. *2021 International Conference on Rebooting Computing (ICRC)*, 56–63.

Rawat, B., Mehra, N., Bist, A. S., Yusup, M., & Sanjaya, Y. P. A. (2022). Quantum computing and ai: Impacts & possibilities. *ADI Journal on Recent Innovation*, *3*(2), 202–207.

Riel, H. (2021). Quantum computing technology. *2021 IEEE International Electron Devices Meeting (IEDM)*, 1–3.

Schatzki, L., Arrasmith, A., Coles, P. J., & Cerezo, M. (2021). Entangled datasets for quantum machine learning. *arXiv preprint arXiv:2109.03400*.

Sharma, M., Choudhary, V., Bhatia, R., Malik, S., Raina, A., & Khandelwal, H. (2021). Leveraging the power of quantum computing for breaking rsa encryption. *Cyber-Physical Systems*, *7*(2), 73–92.

Sheng, Y.-B., & Zhou, L. (2017). Distributed secure quantum machine learning. *Science Bulletin*, *62*(14), 1025–1029.

Steane, A. (1998). Quantum computing. *Reports on Progress in Physics*, *61*(2), 117.

Stock, R., & James, D. F. (2009). Scalable, high-speed measurement-based quantum computer using trapped ions. *Physical review letters*, *102*(17), 170501.

Suzuki, T., & Katouda, M. (2020). Predicting toxicity by quantum machine learning. *Journal of Physics Communications*, *4*(12), 125012.

Weber, J., Koehl, W., Varley, J., Janotti, A., Buckley, B., Van de Walle, C., & Awschalom, D. D. (2010). Quantum computing with defects. *Proceedings of the National Academy of Sciences*, *107*(19), 8513–8518.

Williams, C. P. (2010). *Explorations in quantum computing*. Springer Science & Business Media.

Zaspel, P., Huang, B., Harbrecht, H., & von Lilienfeld, O. A. (2018). Boosting quantum machine learning models with a multilevel combination technique: Pople diagrams revisited. *Journal of chemical theory and computation*, *15*(3), 1546–1559.

Zeuner, J., Pitsios, I., Tan, S.-H., Sharma, A. N., Fitzsimons, J. F., Osellame, R., & Walther, P. (2021). Experimental quantum homomorphic encryption. *npj Quantum Information*, *7*(1), 25.