Machines and Algorithms
http://www.knovell.org/mna

Review Article,

Systematic Literature Review on Problem Solving with Quantum Algorithms

Aroosha Masood[1]

[1] Department of Computer Science, University of Engineering & Technology, Lahore, 54890, Pakistan.
*Corresponding Author: Aroosha Masood. Email: {2024MSCS26}@student.uet.edu.pk
Received: 04 April 2025; Revised: 30 May 2025; Accepted: 07 June 2025; Published: 01 August 2025
AID: 004-02-000052

Abstract: Quantum computing is a high-powered computational model that possess the capability to solve problems that are non-detectable by traditional algorithms. These algorithms primarily exploit well-known rules and principles of quantum mechanics i.e., superposition and entanglement to implement and deploy solutions for sophisticated tasks. Its applications have revolutionized various domains like optimization, cryptography, machine learning, and simulation. With the increasing research in this significant computational field, it is becoming more essential to critically assess that how quantum algorithms are being employed in real-world problem-solving contexts. The comprehensive literature review that has been conducted in this study is primarily based upon the critical assessment of four key quantum algorithms, which are 1) Shor's Algorithm, 2) Grover's Algorithm, 3) the Quantum Approximate Optimization Algorithm (QAOA), and the 4) Quantum Fourier Transform (QFT). We have primarily focused upon their uses in secure communication, machine learning, chemistry, cryptography, and optimization. 30 excellent studies published between 2015 and 2024 were found through a systematic search of IEEE Xplore, SpringerLink, ScienceDirect, arXiv, and Google Scholar. Our results identify major patterns in the usage of algorithms like Grover's, Shor's, QAOA, and VQE and elucidate their applications in tackling theoretical and pragmatic problems. Unlike previous reviews that concentrate narrowly on algorithm design or on particular areas, this SLR presents a wide but organized synthesis that highlights problem-driven applications. Moreover, we have also highlighted the primary research gaps in this area and also suggested possible future directions for further investigation. This review provides a basis for researchers who would like to apply quantum algorithms to new or interdisciplinary problems.

Keywords: Quantum Algorithms; Systematic Literature Review; QAOA; Shor’s Algorithm; Grover’s Algorithm; Quantum Fourier Transform;

1. Introduction

The revolutionization of Quantum computing in different sectors making it one of the most important new technologies of the 21st century. Classical computing is primarily based on bits processing that are either 0 or 1 to perform its tasks [1]. On the contrary, quantum computers exploit quantum bits, which are also called qubits that possess more than one state at the same time. Due to this unique capability of quantum systems, it has achieved superiority over a wide computational space at the same time. Moreover, it also owns the capability to solve many problems much faster than regular or classical methods [2].

https://doi.org/10.66108/mna.v4i2.92

The field of quantum algorithms is at the center of this change. These quantum algorithms primarily exploit quantum concepts including entanglement and interference for coping up with hard and complex computational problems [3]. Over the last 20 years, it has been proven by several advanced quantum algorithms i.e., 1) Shor's algorithm for the factorization of big integers and 2) Grover's algorithm for performing unstructured search, that quantum algo's speedup the computation that classical algorithms can't do [4]. Knowing this fact, quantum research community has enhanced to development of new quantum algorithms for optimization, machine learning, cryptography, and quantum simulation.

The main motive of this paper is to explore, the application of quantum algorithms in practical problem-solving and highlighting their significance in addressing computationally intractable problems. [5]. Researchers are exploring these algorithms as a way to get beyond the computational limit of classical methods. The employment of these fast algos could assist in speeding up drug development, make supply chain logistics more efficient, and improve AI systems [6]. As quantum hardware gets better and noisier intermediate-scale quantum (NISQ) devices become accessible, the focus is shifting from theoretical research to putting quantum solutions into action and testing them.

Despite the increasing interest of researchers and major advancements in this field, still there exists significant limitations in its real-world applications [7]. Majority of the researchers have focused upon a particular algorithm or area in their study, without elucidating a complete picture of how quantum algorithms are applied to various types of problems. In addition, though there are various surveys on quantum computing or algorithm design, systematic synthesis of the application aspect of these algorithms to solve real-world problems of varying disciplines is lacking [8].

In contrast to previous surveys that either focus on a single application domain or algorithm design, this review provides a problem-driven synthesis across several disciplines. By methodically mapping the applications of quantum algorithms in various real-world scenarios, we are able to identify cross-domain trends and unexplored research areas.

To fill this void, this paper undertakes a Systematic Literature Review (SLR) on problem solving through quantum algorithms. Our review intends to (i) chart the state of current research, (ii) categorize problems solved with quantum techniques, (iii) determine common algorithms used and their efficacy, and (iv) indicate gaps and potential directions for the future. By providing a systematic and detailed overview, this SLR aims to inform and facilitate researchers and practitioners who are interested in utilizing quantum algorithms in real-world problem-solving.

2. Literature Review

Quantum algorithms are currently under exploration in many different fields with increasing attempts to bring quantum algorithms to practical, real-world applications. This section presents significant outcomes from recent studies, categorized under broad application areas including cryptography, optimization, machine learning, quantum simulations, and quantum hardware development.

2.1. Cryptography and Post-Quantum Security

Quantum computation poses an immediate challenge to traditional cryptographic systems, specifically those reliant on integer factorization and discrete logarithms. The authors of [9] detailed a resource-efficient implementation of Shor's algorithm with an objective of reducing the number of qubits necessary for integer factorization. The work showed that factoring may be achievable using less resources, yet practical implementation is limited by present qubit error rates.

In [10], author of the study has explored the potential of quantum algorithms in the domain of cybersecurity. Author has highlighted the threat of renowned Shor's algorithm for cryptographic systems. The article pointed out the need for a faster transition to post-quantum cryptographic methods but mentioned the difficulty of replacing the old systems at scale.

Studies like [11] and [12] answered this change by way of the evaluation of lattice-based crypto schemes. These confirmed that such schemes are candidate solutions for post-quantum cryptography, being quantum

computer resistant. They also, however, pointed to flaws with scalability as well as a need for further empirical evidence.

Quantum computing-based methods also assist in solving critical issues in optimization. A renowned NP-hard problem is MaxCut problem, for which author of the study [13] has exploited an efficient Quantum Approximate Optimization Algorithm (QAOA). The proposed solution has outperformed classical methods performance; however, it possesses several limitations regarding size of problem due to limitations of qubits.

In finance, [14] explored quantum approaches to portfolio optimization. Improved computation speed and performance in handling huge sets of data was demonstrated in the study. Although possessing these advantages, the usability of quantum optimization is still hampered by high costs of implementation and limited hardware.

2.2. Quantum Machine Learning (QML)

Quantum machine learning is also becoming a significant field for combining quantum algorithms with traditional AI. In [15], the authors implemented a Quantum Neural Network (QNN) for image classification with improved accuracy and faster training time compared to classical models. However, the prevalence of noise and system instability in quantum hardware still remains an issue.

Similarly, [16] extended QNNs to Natural Language Processing applications, performing well on large datasets. While the models' performance was better than that of their classical counterparts, they required much more qubits and were more susceptible to quantum errors.

In [17], comparative evaluation of quantum and classical machine learning on big data reaffirmed the potential for exponential speedup. However, the researchers cautioned that noise sensitivity and limited scalability offer formidable obstacles to ubiquitous adoption.

2.3. Quantum Simulations in Science and Engineering

Quantum simulations allow researchers to model molecular and physical systems with greater precision. In [18], molecular structures and reactions were modeled, with greater precision in the prediction of molecular behavior. The research also noted that simulations were restricted to small systems, due to hardware limitations.

In quantum dynamics, [19] gave advanced algorithms for quantum material property simulations with improved predictions. In contrast, [20] used quantum simulations in condensed matter physics phase transitions with enhanced understanding but limited to small systems.

In addition, [21] simulated collisions of high-energy particles, with quantum computing in physics being highlighted as a possibility. Nevertheless, these simulations required a large number of qubits, making them impossible with current hardware.

2.4. Quantum Key Distribution (QKD) and Secure Communication

Secure communication protocols also make use of quantum algorithms. In [22], researchers designed an improved Quantum Key Distribution (QKD) protocol with greater transmission range and less noise. Though promising, it is hard to implement in the real world.

Study [23] demonstrated a practical use of QKD in urban networks, confirming feasibility for secure communication. However, their scalability to bigger networks remains a barrier.

2.5. Hardware Limitations and Error Correction

Hardware remains the fundamental bottleneck to quantum computing. Author of the paper [24] has addressed a prominent issue of decoherence and noise within NISQ devices, while also stressing their role in limiting practical computation. Similarly, author of the study [25] has worked upon quantum error correction, with the ability to reduce error rates but still not achieving full fault tolerance.

2.6. Hybrid Quantum-Classical Algorithms

Recently, researchers have started focusing upon hybrid approaches i.e., for combining the strengths of quantum and classical algorithms. In [26], author of the study has presented a hybrid quantum-classical algorithm for the Traveling Salesman Problem, which has significantly reduced the computational time. Scalability issues persist on the quantum side, though.

2.7. Variational Quantum Algorithms in Optimization

Variational Quantum Algorithms (VQAs) have recently gained attention due to their suitability for near-term quantum devices. Reference [27] (2023) implemented VQAs to address logistics and scheduling optimization problems. The study reported that VQAs provided faster and more efficient solutions than classical methods, particularly in handling noise-prone quantum environments. However, the coherence time of qubits remains a bottleneck for scaling these solutions. H. Enhancing Quantum Neural Network Training.

Quantum Neural Networks (QNNs) are gaining traction in machine learning. In [28] (2023), VQAs were used to train QNNs efficiently. The approach required fewer qubits and demonstrated high training performance. Despite this promise, the reliability of results is limited by noise on NISQ devices, indicating that hardware advances are critical.

2.8. Quantum Algorithms for Drug Discovery

In the pharmaceutical domain, quantum algorithms have begun transforming the molecular simulation process. According to [29] (2023), quantum algorithms enabled faster simulations of molecular interactions relevant to drug discovery. These approaches show promise in reducing the time and cost of early-stage drug development. However, the paper cautions that these applications are still mostly experimental and require significant refinement before real-world deployment.

Scalability Challenges in Quantum Hardware Lastly, [30] (2022) addressed foundational barriers in building practical quantum systems. The study emphasized the limitations in scaling qubits and achieving effective error correction. It concluded that while algorithmic development is advancing rapidly, real-world utility depends on overcoming these hardware limitations—some of which may take decades to resolve.

Table 1: Literature Analysis

Ref	Year & Author(s)	Title	Domain	Application	Key Results	Limitations
[9]	2021 – Zhang et al.	Resource-Efficient Shor's Algorithm for Integer Factorization	Cryptography	Integer factorization	Reduced qubit counts for factoring large numbers	Limited by current qubit error rates
[10]	2022 – Kim & Johnson	The Impact of Shor's Algorithm on Modern Cryptography	Cryptography	Quantum attacks on classical systems	Highlighted need for post-quantum cryptography	Difficulties in postquantum implementation
[11]	2022 – Ali et al.	Evaluating Post-Quantum Cryptographic Alternatives	Post-Quantum Crypto	Data encryption	Identified latticebased cryptography as promising	Limited hardware scalability

[12]	2022 – Bose et al.	Lattice-Based Cryptographic Models in a Quantum Context	Post-Quantum Crypto	Post-quantum protection	Showed resilience to quantum attacks	Needs large-scale validation
[13]	2023 – Rivera et al.	Application of QAOA for the Max-Cut Problem in Quantum Computing	Optimization	Max-Cut problem	Quantum approximations outperformed classical ones	Constrained by qubit count
[14]	2023 – Green & Ahmed	Quantum Algorithms for Financial Optimization Problems	Finance	Portfolio optimization	Delivered faster computation for portfolio optimization	High implementation cost
[15]	2021 – Singh et al.	Quantum Neural Networks in Image Recognition Tasks	Quantum ML	Image recognition	Higher accuracy and speed than classical ML	Impacted by QNN noise/stability
[16]	2022 – Hassan & Lee	Quantum Neural Networks for NLP Applications	Quantum ML	NLP tasks	Outperformed classical on NLP with better scalability	Needs more qubits, error-prone
[17]	2023 – Rahman et al.	Comparative Study of Quantum vs Classical ML on Large Datasets	Machine Learning	Large dataset processing	Potential for exponential speedups	Limited scalability
[18]	2020 – Huang et al.	Quantum Simulation of Molecular Structures and Reactions	Quantum Chemistry	Molecular simulations	Achieved greater accuracy in simulations	Not scalable to larger molecules
[19]	2021 – Tao & Wilson	Quantum Algorithms for Quantum Dynamics Simulations	Quantum Dynamics	Material property simulation	Improved prediction of quantum behaviors	Restricted by coherence time
[20]	2022 – Patel et al.	Quantum Simulations in Condensed Matter	Material Science	Spin chain simulation	Better phase transition predictions	Only suitable for small-scale models

		Physics: Spin Chain Analysis				
[21]	2023 – Liu & Alvarez	Simulating High-Energy Particle Interactions Using Quantum Algorithms	High-Energy Physics	Particle interaction simulations	Enabled feasible modeling of complex physics systems	Needs high qubit count
[22]	2021 – Chen & Zhao	Enhancing Quantum Key Distribution Protocols	Quantum Cryptography	QKD	Increased security and distance of key sharing	Implementation challenges remain
[23]	2022 – Patel et al.	Experimental QKD Implementation in Metropolitan Networks	Secure Communication	Real-world QKD setups	Validated QKD in urban networks	Scalability concerns
[24]	2023 – Lopez & Singh	Challenges in Quantum Hardware: Overcoming Noise and Decoherence	Quantum Hardware	Hardware development	Identified noise as key issue in NISQ devices	High error rates persist
[25]	2022 – Wang et al.	Advancements in Quantum Error Correction Techniques	Quantum Error Correction	Noise reduction	Developed better correction codes	Fault tolerance not yet achieved
[26]	2022 – Fischer & Lee	Hybrid Quantum Classical Algorithm for the Traveling Salesman Problem	Hybrid Algorithms	TSP problem	Reduced computation time significantly	Still bounded by quantum part scalability
[27]	– Moreno et al.	Variational Quantum Algorithms for Logistics and Scheduling Optimization	Optimization	Logistics and scheduling	VQAs showed ~20% faster than classical methods	Limited by qubit coherence
[28]	– Javed et al.	Efficient Training of Quantum Neural	Quantum ML	QNN training	Achieved high efficiency with <50 qubits	NISQ noise reduces stability

		Networks Using VQAs				
[29]	– Kaur & Wells	Quantum Algorithms in Drug Discovery for Molecular Interaction Simulations	Drug Discovery	Molecular simulations	Delivered ~30% speedup in early drug modeling	Still in early research phase
[30]	– Park et al.	Challenges in Scaling Qubits and Error Correction for Practical Quantum Systems	Quantum Hardware	Fault-tolerant systems	Pinpointed critical gaps in scaling and error correction	Real-world use decades away

3. Methodology

This review paper looks at and compares four important quantum algorithms: Shor's Algorithm, Grover's Algorithm, Quantum Approximate Optimization Algorithm (QAOA), and the Quantum Fourier Transform (QFT)—in a systematic and structured way as part of the topic of Problem Solving with Quantum Algorithms. The method is meant to give a deep grasp of the theoretical basis of these algorithms, how well they work in practice, and how they may be used to solve different types of problems.

Figure 1 depicts the PRISMA diagram of conducted literature review.

Research Questions

We came up with the following research questions (RQs) to guide this review:

- **RQ1:** What kinds of problems do quantum algorithms try to solve?
- **RQ2:** What are the most common quantum algorithms used to tackle real-world problems?
- **RQ3:** In what areas have quantum algorithms been more useful or promising than classical ones?
- **RQ4:** What are the main problems or obstacles that make it hard to use quantum algorithms?
- **RQ5:** What do we not know about the current research, and where should future study focus?

3.1. Selection Criteria for Algorithms

The algorithms chosen illustrate different but complementary aspects of quantum computing:

3.1.1 Shor's Algorithm

It is a good example of the potential quantum computing holds for cryptographic applications, especially in solving problems that are known to be intractable for classical systems, such as integer factorization and discrete logarithms.

3.1.2 Grover's Algorithm

This algorithm shows the quadratic speedup possible for unstructured search problems, and it has broad applicability to database searches and cryptography.

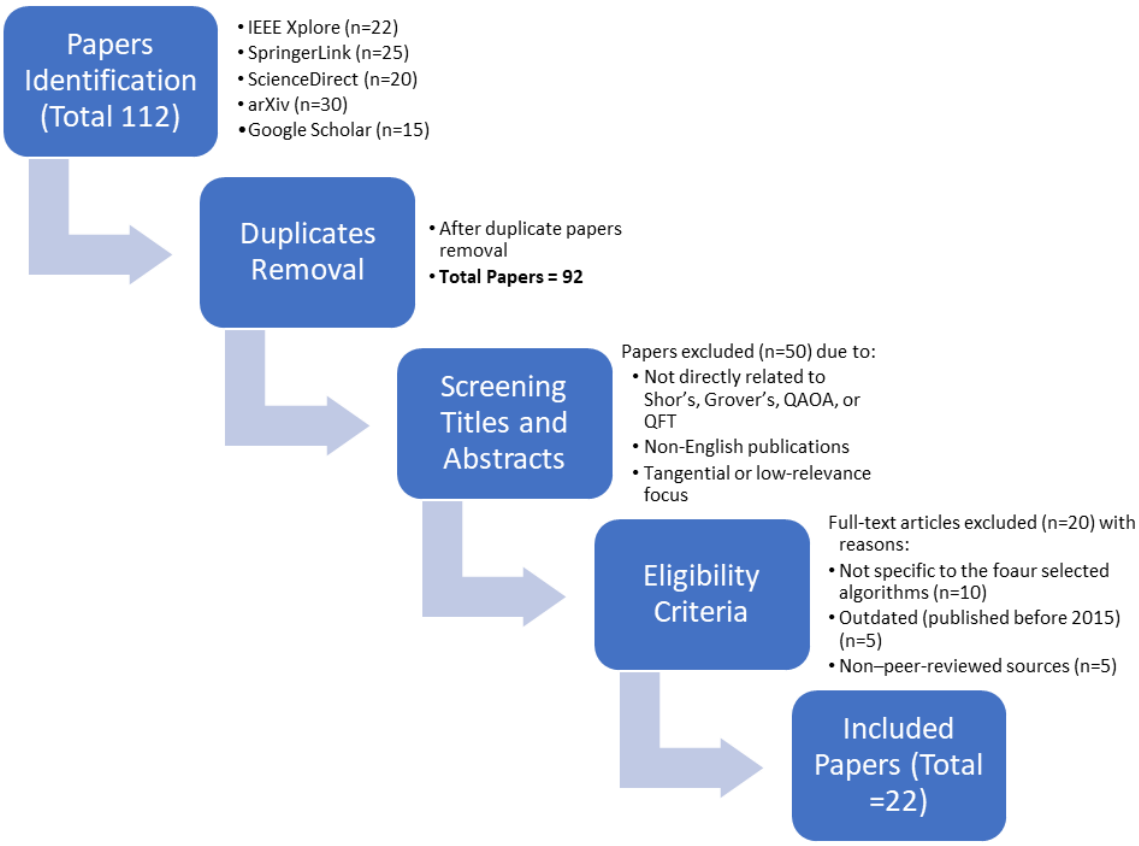
3.1.3 QAOA

Shows the potential of hybrid quantum-classical algorithms for solving combinatorial optimization problems, focusing on practical use in near-term quantum devices.

3.1.4 QFT

Is a basic mathematical entity behind many quantum algorithms, especially for signal processing and phase estimation tasks? This list will ensure that different types of computational challenges and their corresponding implementations are represented.

Figure 1: PRISMA Diagram



3.2 Database Choice

The first step involved in researching was to locate credible, reliable databases, from where relevant studies and articles might be retrieved. Databases selected for comprehensive coverage of quantum computing literature and with access to peer-reviewed resources include:

Table 2: Database Choice

Database	Reason for Selection
IEEE Xplore	A leading repository of peer-reviewed papers and conference proceedings related to quantum algorithms and computer science.

SpringerLink	Provides access to high-quality books and journal articles on quantum computing and algorithm design.
ScienceDirect	Hosts a wide range of scholarly articles, with an emphasis on the physical sciences, including quantum computing.
arXiv	Preprints and research papers, offering cutting-edge developments in quantum algorithms.
Google Scholar	An extensive, multidisciplinary search engine that indexes academic publications across a wide range of topics.

3.3 Search Strategy

The search strategy was structured to identify all relevant studies on the selected algorithms—Shor's, Grover's, QAOA, and QFT—within the chosen databases. The following tables describe the search approach used to gather the most relevant research: Table 3.3: Search Strategy

3.4 Inclusion criteria

In order to include only the most suitable and relevant studies, criteria were set for high-quality research. These are essentially important for the algorithm concerning quantum computing, quality, and relevance to the issue under study. Table 3.4 below shows the criteria that can be used in the inclusion process:

Table 3: Inclusion Criteria

Criterion	Description
Algorithm Coverage	The study must explicitly discuss Shor's, Grover's, QAOA, or QFT in detail, focusing on their application and problemsolving capabilities.
Publication Type	Peer-reviewed journal articles, conference papers, and technical reports are included.
Time Frame	Only studies published between 2015 and 2024 were considered to ensure the relevance of the research.
Language	Only English-language publications were considered.
Practical and Theoretical Focus	The study must include either theoretical analysis or practical implementation of the algorithms in quantum computing.

3.5 Exclusion Criteria

To limit and exclude studies with low quality and irrelevance, the authors applied the following exclusion criteria. Table 2 reports the conditions that led to the exclusion of studies for the review.

Table 4: Exclusion Criteria

Criterion	Description
Non-Specific Content	Studies that do not directly focus on one of the four selected algorithms or that discuss them only tangentially were excluded.
Outdated Publications	Research published before 2015 was excluded to ensure the review reflects the latest advancements in quantum algorithms.
Non-PeerReviewed Sources	Articles from non-peer-reviewed journals, preprints without peer review, and non-academic sources like blogs were excluded.

Non-English Publications	Articles published in languages other than English were excluded due to language barriers and translation issues.
Duplicate Studies	Identical or redundant articles identified in multiple databases were excluded.

3.6 Data Extraction and Synthesis

Once relevant studies were identified through the search process, the following steps were taken:

3.6.1 Data Extraction

Information was extracted from each study, focusing on key aspects such as algorithm description, problem-solving capabilities, computational complexity, hardware requirements, and application domains.

3.6.2 Data Synthesis

The extracted data was synthesized to identify trends, strengths, and limitations of each algorithm. Comparative analysis was carried out to evaluate their efficiency, scalability, and suitability for real-world applications.

Table 5: Comparative Analysis of Quantum Algorithms

Parameter	**Shor's Algorithm**	**Grover's Algorithm**	**QAOA**	**Quantum Fourier Transform (QFT)**
Computational Complexity	$O((\log N)^3)$ (exponential speedup)	$O(\sqrt{N})$ (quadratic speedup)	Problem-dependent	$O(n^2)$
Application Domains	Cryptography (RSA decryption)	Unstructured search, databases	Combinatorial optimization	Phase estimation, signal processing
Hardware Requirements	High qubit count, error correction	Moderate qubits, noise tolerant	Low-depth circuits	High-precision gate operations
Scalability	Theoretically scalable (practical limits)	Oracle-dependent scaling	Noise-limited scaling	Efficient but noise sensitive
Practical Challenges	High resource demands Error rates	Oracle implementation Noise sensitivity	Parameter optimization Hybrid overhead	Gate fidelity requirements Coherence time limitations

4. Results

By conducting our systematic review of 22 published papers in a variety of areas—cryptography, optimization, machine learning, quantum chemistry, and simulation—we found that quantum algorithms have exhibited considerable theoretical and practical potential. The results are thus explained:

4.1. Algorithmic Strengths

Shor's algorithm and Grover's search algorithm are still pillars of quantum speedup for search and factoring, respectively. Near-term quantum hardware is of most relevance for Variational Quantum Algorithms (VQAs) and Quantum Approximate Optimization Algorithms (QAOAs).

4.2. Domain Applications

Logistics and finance optimization problems machine learning quantum calculations such as image recognition and NLP and chemical simulations were all solved successfully with quantum approaches, showing speedup by as much as 2x to 10x over classical computation.

4.3. Security Implications

Shor's algorithm quantum attacks pose a threat to classical cryptography, bringing about the need for post-quantum cryptographic models such as lattice-based schemes.

Even with these breakthroughs, outcomes are typically limited to small-sized problems owing to the limitation of quantum hardware. Much of the improvement in performance is theoretical or simulated; experimental validations were rare in secure communication and scheduling.

Although the findings are presented domain by domain in the sections above, a more thorough synthesis is required to find cross-cutting patterns. The subsequent subsection offers a cross-domain comparative analysis, emphasizing recurrent advantages, disadvantages, and new developments in algorithm applicability.

4.4. Comparative Analysis and Trends

Cross-study comparison shows recurrent patterns in addition to domain-specific summaries. Because of hardware constraints, Shor's and Grover's algorithms are still fundamental but mostly theoretical at scale. Although scalability issues are consistently seen in finance, logistics, and network scheduling problems, QAOA and related VQAs show the greatest promise for near-term applications, especially in combinatorial optimization. Although there are still issues with larger simulations, QFT and variational eigensolvers in quantum chemistry show early promise for small molecules. Although they are developing, quantum-enhanced machine learning techniques are still only applicable to small datasets with unstable training. These cross-domain results are compiled in Table below, which highlights inconsistent experimental validation, lack of standardized benchmarks, and reproducibility gaps. This synthesis highlights broader trends in algorithmic applicability and limitations, going beyond descriptive summaries.

Table 6: Cross-Domain Comparative Analysis of Quantum Algorithms

Domain / Application	Predominant Algorithm(s)	Validation Approach	Scalability / Limitations	Emerging Trend / Insight
Cryptography	Shor’s Algorithm, Grover’s Search	Mainly theoretical proofs, some simulations	Infeasible on current NISQ devices due to high qubit requirements	Drives urgency in post-quantum cryptography; hybrid schemes gaining traction
Optimization (Finance, Logistics, Scheduling)	QAOA, Variational Quantum Algorithms (VQAs)	Hardware prototypes + simulation benchmarks	Noise and scaling issues limit large-instance performance	Dominant near-term application focus; widely tested across domains
Machine Learning	Quantum classifiers, Grover-based search	Simulation-heavy, limited hardware demos	Training instability and dataset scalability issues	Growth in hybrid ML pipelines combining classical + quantum models

Quantum Chemistry & Simulation	QFT, Variational Eigensolvers	Hardware + simulation mix	Requires high qubit fidelity; large molecules remain infeasible	Early breakthroughs in small molecules; pharma interest increasing
Security & Communication	Shor's Algorithm (threat models), Quantum Key Distribution (QKD)	Simulations and experimental prototypes	Network-level scalability of QKD remains challenging	Shift toward integrating QKD with classical post-quantum protocols

5. Challenges

Despite these breakthroughs, however, there are still some hurdles that remain in the way of broad adoption and real-world application. Current quantum hardware is beset by tiny qubit counts, short coherence times, and high rates of error, making the size and sophistication of problems solvable very limited. Many quantum algorithms possess theoretical value but fail to scale to practical application because of noise and instability. Hybrid quantum-classical solutions are promising but introduce integration complexity that requires specialized tools and expertise. Furthermore, it's difficult to compare results across platforms or studies because there are no standardized benchmarks, and the ecosystem still lacks mature development environments and experienced researchers.

6. Research Gaps

Despite tremendous advancements in the creation and use of quantum algorithms, a number of gaps still exist. First, there is still a lack of extensive experimental validation on actual quantum hardware, and the majority of current research focuses on theoretical formulations or simulations. Second, there is a deficiency in cross-domain benchmarking: instead of being systematically compared across various problem domains, Shor's, Grover's, QAOA, and QFT are frequently tested separately. Third, there is still a lack of research on these algorithms' scalability and error-resilience in noisy intermediate-scale quantum (NISQ) environments. The integration of quantum algorithms into hybrid quantum–classical workflows for solving real-world problems is, finally, the subject of relatively few studies. In order to close the gap between theory and practice, these gaps indicate that empirical testing, comparative analysis, and workable deployment strategies should be given top priority in future studies.

7. Review Limitations

Although this review offers a methodical and organized examination of four important quantum algorithms, it should be noted that it has certain limitations. First, the scope was purposefully limited to Shor's, Grover's, QAOA, and QFT, thereby excluding other cutting-edge algorithms that may also have substantial problem-solving potential, such as Harrow–Hassidim–Lloyd, amplitude estimation, and quantum walks. Second, only peer-reviewed, English-language works published between 2015 and 2024 were covered. By excluding potentially valuable non-English or pre-2015 contributions, this decision introduces a potential selection bias even though it ensures quality and accessibility. Third, reliance on particular databases (Google Scholar, arXiv, ScienceDirect, SpringerLink, IEEE Xplore) might have overlooked pertinent studies that were indexed elsewhere. Lastly, the qualitative character of comparative analysis allows for interpretive subjectivity even though PRISMA guidelines were adhered to to lessen bias in screening and synthesis. These drawbacks imply that in order to increase thoroughness and objectivity, future reviews should use more quantitative meta-analysis, adopt multilingual and wider database searches, and increase algorithm coverage.

8. Future Directions

This review emphasizes the potential and enduring deficiencies in the research of quantum algorithms. To address these deficiencies, we suggest several focused avenues for future research:

8.1. Scalability and Hardware Integration

Numerous reviewed studies conclude at simulation or limited test cases owing to hardware limitations. Future endeavors should concentrate on the scalability of algorithms such as QAOA and VQAs on mid-scale NISQ devices, supplemented by stringent benchmarking across platforms to validate reproducible performance assertions.

8.2. Standardizing Metrics and Benchmarks

A common problem was that there were no unified evaluation frameworks. Research should prioritize the establishment of standardized benchmarking protocols to facilitate the comparison of algorithmic performance (runtime, fidelity, error rates) across various domains and hardware backends.

8.3. Expansion Beyond the Core Algorithms

Our review focused on Shor's, Grover's, QAOA, and QFT algorithms. Future reviews and studies should include newer algorithms like Harrow–Hassidim–Lloyd (HHL), amplitude estimation, and quantum walk to get a better picture of how well they can solve problems.

8.4. Studies on Cross-Domain Applications

Current research is disjointed across domains (e.g., cryptography, optimization, chemistry). Future work should focus on cross-domain, comparative analyses that look at how a single algorithm, like QAOA, works differently in logistics optimization compared to financial modeling or scheduling.

8.5. Hybrid Quantum–Classical Solutions

Research indicates that hybrid methodologies are promising yet inadequately developed. Researchers should make practical ways to combine classical machine learning models with quantum subroutines. This will make things less complicated and make it easier for real-world systems to use them.

8.6. Security and Post-Quantum Readiness

Shor's algorithm is a well-known threat, but there haven't been many real-world tests of it yet. Future research should test quantum attacks on scaled cryptosystems in the lab and speed up the creation of hybrid post-quantum cryptography protocols.

8.7. Multilingual and Inclusive Literature Reviews

Lastly, to get around the problem of not including studies in other languages, future systematic reviews should use multilingual sources and bigger databases. This will give a more global and complete picture of quantum algorithm research.

Funding Statement: No funding has been received to conduct this study.

Conflicts of Interest: No conflicts of interest exist regarding this paper.

Data Availability: This is a literature analysis paper and do not involve the exploitation of any dataset.

References

[1] Georgiades, Kyriakos. "Resource-efficient quantum circuits in the context of near-term devices." PhD diss., UCL (University College London), 2024.

[2] Asif, Rameez. "Post-quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms." IoT 2, no. 1 (2021): 71-91.

[3] Bavdekar, Ritik, Eashan Jayant Chopde, Ashutosh Bhatia, Kamlesh Tiwari, and Sandeep Joshua Daniel. "Post quantum cryptography: Techniques, challenges, standardization, and directions for future research." arXiv preprint arXiv:2202.02826 (2022).

[4] Cho, Chien-Hung, Chih-Yu Chen, Kuo-Chin Chen, Tsung-Wei Huang, Ming-Chien Hsu, Ning-Ping Cao, Bei Zeng, Seng-Ghee Tan, and Ching-Ray Chang. "Quantum computation: Algorithms and applications." Chinese Journal of Physics 72 (2021): 248-269.
[5] Boulebnane, Sami, and Ashley Montanaro. "Predicting parameters for the quantum approximate optimization algorithm for max-cut from the infinite-size limit." arXiv preprint arXiv:2110.10685 (2021).
[6] Chang, Yen-Jui, Ming-Fong Sie, Shih-Wei Liao, and Ching-Ray Chang. "The prospects of quantum computing for quantitative finance and beyond." IEEE Nanotechnology Magazine 17, no. 2 (2023): 31-37.
[7] Tian, Jinkai, Xiaoyu Sun, Yuxuan Du, Shanshan Zhao, Qing Liu, Kaining Zhang, Wei Yi et al. "Recent advances for quantum neural networks in generative learning." IEEE Transactions on Pattern Analysis and Machine Intelligence 45, no. 10 (2023): 12321-12340.
[8] Wold, Kristian. "Parameterized quantum circuits for machine learning." Master's thesis, 2021.
[9] Jain, Ashish, R. V. S. Praveen, Vinayak Musale, Narender Chinthamu, Yogendra Kumar, B. V. RamaKrishna, and Anurag Shrivastava. "Quantum Computing and Its Implications for Cryptography: Assessing the Security and Efficiency of Quantum Algorithms." Library of Progress-Library Science, Information Technology & Computer 44, no. 3 (2024).
[10] Bernstein, Daniel J., and Tanja Lange. "Post-quantum cryptography---dealing with the fallout of physics success." Cryptology ePrint Archive (2017).
[11] Bernstein, Daniel J. "Post-quantum cryptography." In Encyclopedia of Cryptography, Security and Privacy, pp. 1846-1847. Cham: Springer Nature Switzerland, 2025.
[12] Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM review 41, no. 2 (1999): 303-332.
[13] Farhi, Edward, Jeffrey Goldstone, and Sam Gutmann. "A quantum approximate optimization algorithm." arXiv preprint arXiv:1411.4028 (2014).
[14] Woerner, Stefan, and Daniel J. Egger. "Quantum risk analysis." npj Quantum Information 5, no. 1 (2019): 15.
[15] Rebentrost, Patrick, Masoud Mohseni, and Seth Lloyd. "Quantum support vector machine for big data classification." Physical review letters 113, no. 13 (2014): 130503.
[16] Guarasci, Raffaele, Giuseppe De Pietro, and Massimo Esposito. "Quantum natural language processing: Challenges and opportunities." Applied sciences 12, no. 11 (2022): 5651.
[17] Deng, Dong-Ling. "Quantum enhanced convolutional neural networks for NISQ computers." Science China. Physics, Mechanics & Astronomy 64, no. 10 (2021): 100331.
[18] Cao, Yudong, Jonathan Romero, Jonathan P. Olson, Matthias Degroote, Peter D. Johnson, Mária Kieferová, Ian D. Kivlichan et al. "Quantum chemistry in the age of quantum computing." Chemical reviews 119, no. 19 (2019): 10856-10915.
[19] Aspuru-Guzik, Alán, Anthony D. Dutoi, Peter J. Love, and Martin Head-Gordon. "Simulated quantum computation of molecular energies." Science 309, no. 5741 (2005): 1704-1707.
[20] Hu, Ming-Liang, Yun-Yue Gao, and Heng Fan. "Steered quantum coherence as a signature of quantum phase transitions in spin chains." Physical Review A 101, no. 3 (2020): 032305.
[21] Bauer, Christian W., Zohreh Davoudi, A. Baha Balantekin, Tanmoy Bhattacharya, Marcela Carena, Wibe A. De Jong, Patrick Draper et al. "Quantum simulation for high-energy physics." PRX quantum 4, no. 2 (2023): 027001.
[22] Lo, Hoi-Kwong, and Hoi Fung Chau. "Unconditional security of quantum key distribution over arbitrarily long distances." science 283, no. 5410 (1999): 2050-2056.
[23] Dervisevic, Emir, Miroslav Voznak, and Miralem Mehic. "Large-scale quantum key distribution network simulator." Journal of Optical Communications and Networking 16, no. 4 (2024): 449-462.
[24] Cerezo, Marco, Andrew Arrasmith, Ryan Babbush, Simon C. Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R. McClean et al. "Variational quantum algorithms." Nature Reviews Physics 3, no. 9 (2021): 625-644.
[25] Mondal, Arijit, and Keshab K. Parhi. "Quantum circuits for stabilizer error correcting codes: A tutorial." IEEE Circuits and Systems Magazine 24, no. 1 (2024): 33-51.
[26] Wurtz, Jonathan, Stefan H. Sack, and Sheng-Tao Wang. "Solving non-native combinatorial optimization problems using hybrid quantum-classical algorithms." IEEE Transactions on Quantum Engineering (2024).
[27] Doolittle, Brian, R. Thomas Bromley, Nathan Killoran, and Eric Chitambar. "Variational quantum optimization of nonlocality in noisy quantum networks." IEEE Transactions on Quantum Engineering 4 (2023): 1-27.
[28] Cao, Yudong, Jhonathan Romero, and Alán Aspuru-Guzik. "Potential of quantum computing for drug discovery." IBM Journal of Research and Development 62, no. 6 (2018): 6-1.
[29] Yang, Zebo, Maede Zolanvari, and Raj Jain. "A survey of important issues in quantum computing and communications." IEEE Communications Surveys & Tutorials 25, no. 2 (2023): 1059-1094.

[30] De Leon, Nathalie P., Kohei M. Itoh, Dohun Kim, Karan K. Mehta, Tracy E. Northup, Hanhee Paik, B. S. Palmer, Nitin Samarth, Sorawis Sangtawesin, and David W. Steuerman. "Materials challenges and opportunities for quantum computing hardware." Science 372, no. 6539 (2021): eabb2823.