International Journal of Science and Technology (IJST)
ISSN: 3049-1118, Volume- 3, Issue- 4 (October - December 2026)

A Comprehensive Review of Quantum Computing: Theoretical Foundations, Hardware Architectures, and Present-Era Challenges

Priyanka M C S
PG Department of Computer Applications, Nehru Memorial College (Autonomous)
Puthanampatti, Tiruchirappalli, Tamil Nadu, India - 621007

ABSTRACT

Quantum computing represents a foundational paradigm shift from traditional classical computational models, leveraging the intrinsic mechanics of quantum physics—specifically superposition, entanglement, and unitary interference—to execute parallel processing frameworks at an exponential operational scale. This state-of-the-art review systematically deconstructs the mathematical framework of quantum bit (qubit) state vectors within complex Hilbert spaces and details pioneering algorithms like Shor's and Grover's operations. Furthermore, we evaluate dominant contemporary hardware frameworks, specifically contrasting superconducting circuits against trapped-ion architectures across critical indices of coherence metrics, operational speeds, and thermal constraints. Finally, this review highlights systemic algorithmic barriers including phase-flip/bit-flip noise profiles, decoherence phenomena, and real-world deployment challenges across cryptographic infrastructure and biochemical modeling matrices, charting the roadmap from Noisy Intermediate-Scale Quantum (NISQ) systems toward scalable, fault-tolerant ecosystems.

Keywords: quantum computing, qubits, superposition, nisq era, cryptography, trapped-ion

1. INTRODUCTION

Quantum technology marks an unprecedented multidisciplinary evolution bridging complex mathematics, physical quantum mechanics, and contemporary computation theory. While traditional systems encode standard variables via deterministic binary logic configurations (bounded strictly to static 0 and 1 bit registers), quantum computational environments process multi-state registers utilizing complex probability amplitudes. By utilizing multi-dimensional complex Hilbert spaces, a single quantum bit—or qubit—can manipulate linear spatial equations simultaneously before triggering state collapse during terminal physical measurement operations. This fundamental architectural modification dramatically accelerates computational data throughput, making highly complicated structural matrices manageable.

The rise of quantum frameworks is not simply an incremental speedup of classical computing architectures but a structural reinvention of how information is stored, manipulated, and

*Corresponding Author Email: priyankachandran190804@gmail.com
Published: 10 October 2026
DOI: https://doi.org/10.70558/IJST.2026.v3.i4.241334
Copyright © 2026 The Author(s). This work is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0).

retrieved. Classical systems scale linearly with the addition of logical bits, meaning that doubling the input power requires doubling the underlying transistors. Conversely, quantum systems scale exponentially, allowing a register of relatively few high-fidelity qubits to maintain a state space that exceeds the number of atoms in the observable universe. This mathematical scaling unlocks computational possibilities that would require classical supercomputers to run for billions of years, effectively redefining the boundary between tractable and intractable computational problems.

1.1. Research Objectives

The foundational trajectory of this exhaustive review is structured along a systematic analysis pattern: (i) analyze the exact linear algebraic modeling defining multi-qubit tensor networks; (ii) investigate operational performance attributes separating major hardware systems; (iii) critique physical limitations governing operational noise and environmental decoherence vector properties; and (iv) assess the deployment mechanics of quantum-resistant security protocols alongside molecular optimization arrays designed to process complex algorithmic logic paths.

2. LITERATURE REVIEW

The theoretical blueprint for leveraging quantum mechanical attributes for operational processing tasks was originally structured by Nielsen and Chuang [1], detailing standard linear equations for state vector transformations. Subsequent computational research highlighted the role of quantum parallelism arrays in executing fast mathematical processing configurations over dense search frameworks [2]. However, real-world implementation challenges emerge when scaling system physical sizes. Preskill [3] established critical criteria defining the limitations of Noisy Intermediate-Scale Quantum (NISQ) frameworks, emphasizing how ambient noise affects gate accuracy parameters. Practical educational architectures and software instructions compiled by Smith et al. [4] and Garcia et al. [5] demonstrated optimized models for basic circuit executions, though hardware scaling factors remain bounded by physical environmental variables. Comprehensive historic overviews by Kumar and Singh [6] trace cloud-accessible quantum deployment scales, whereas structural hardware models proposed by Chiang and Frank [8] evaluate the cryogenic infrastructures mandatory for processing tasks without thermal error inflation. Applied computational use cases mapping specialized optimization arrays across biochemical modeling layers and machine learning networks have been thoroughly analyzed by Hidary [9] and structured via systematic lecture datasets compiled by Williams [7] and Kepe [10]. Additional historical and fault-tolerant frameworks established by Kitaev [11], Shor [12], Grover [13], and Bennett & Brassard [14] demonstrate foundational processing benchmarks, while modern industrial platforms highlighted by Arute et al. [15] and Ladd et al. [16] detail scaling dynamics on live test environments.

Recent literature has shifted from pure theoretical abstractions to practical hardware validation and benchmarking. The documentation of quantum supremacy by Arute et al. [15] triggered an intense global race to improve physical gate fidelities beyond the fault-tolerance threshold. Scholars like Bravyi and Kitaev [19] have focused heavily on standardizing topological codes,

identifying specific surface code orientations that can withstand higher internal noise profiles. Furthermore, researchers are exploring intermediate hybrid frameworks where classical co-processors handle optimization tasks while the quantum processing unit (QPU) executes specific subroutines, minimizing the window where decoherence can degrade active calculations. This intersection of classical engineering and quantum mechanics represents the core of modern research, seeking to bridge the gap between contemporary experimental platforms and fully realized scalable computing systems.

3. METHODOLOGY & THEORETICAL FOUNDATIONS

This study utilizes an integrated analytical framework, tracking documented experimental data parameters across physical computing platforms. The foundational element of a single qubit state vector is mathematically defined as an exact linear combination mapping across specific orthogonal basis matrices, denoted as:

$$\psi = \alpha|0\rangle + \beta|1\rangle \quad (1)$$

where α and β represent complex probability amplitudes subject to strict state normalization boundary criteria, satisfying the mathematical relation:

$$|\alpha|^2 + |\beta|^2 = 1 \quad (2)$$

When a system scales to group n-qubits simultaneously, the aggregate operational state space expands exponentially according to a 2^n dimensionality factor, enabling the system to evaluate dense algorithmic trees concurrently.

3.1. Superposition, Entanglement, and Unitary Evolution

Superposition allows quantum registers to sustain complex probabilistic values prior to definitive measurement. This operational capacity is enhanced by quantum entanglement, a localized state where joint systems form non-factorizable structures, mathematically defined via Bell states such as:

$$|\Phi\rangle = (1/2)(|00\rangle + |11\rangle) \quad (3)$$

Any sequential operation acting on these qubits must follow rigorous reversible unitary conditions handled via specific matrices (U), ensuring that total data fidelity metrics are completely sustained throughout the computing process without data leakage:

$$\psi' = U\,\psi \quad (4)$$

The maintenance of unitary evolution is central to quantum information theory. Because any valid quantum logic gate must be represented as a unitary operator, the transformation preserves the inner product of the state space, ensuring that the total probability remains exactly equal to one. Physically, this means that quantum information cannot be inadvertently destroyed or created during an isolated calculation. However, maintaining this strict mathematical isolation in physical hardware requires keeping the system entirely decoupled from the macroscopic environment, an extraordinarily difficult engineering feat due to the constant threat of thermal and electromagnetic disruptions.

4. QUANTUM ALGORITHMS AND ERROR CORRECTION

Advanced quantum architectures leverage specialized circuits to resolve complex mathematical operations that remain intractable for classical processors. Shor's algorithm provides sub-exponential factoring capabilities that compromise RSA encryption protocols [12], while Grover's search optimization condenses database query complexities from O(N) down to an absolute O(√N) threshold [13]. However, sustaining these processes requires robust error mitigation frameworks. Due to the strict constraints of the no-cloning theorem, standard bit-replication schemes are inapplicable. Quantum Error Correction (QEC) protocols overcome this limitation by distributing single logical data channels across multi-qubit entangled states, such as three-qubit bit-flip configurations:

$$|0_L\rangle = |000\rangle, \ |1_L\rangle = |111\rangle \quad (5)$$

This multi-qubit alignment allows syndrome measurement networks to isolate and correct independent bit-flip or phase-flip variations without destabilizing the core quantum information layer [19]. Other specialized dynamic tracking optimization layers like QAOA [17] and VQE [18][20] demonstrate processing improvements inside modern hybrid runtime architectures.

The implementation of fault tolerance relies on the scaling of physical-to-logical qubit ratios. Because individual physical qubits are highly prone to environmental degradation, a single 'logical' qubit—the stable unit used in complex mathematical calculations—must be constructed from an array of hundreds or even thousands of highly entangled physical qubits. These physical components work in unison to continuously run background error-checking procedures, known as syndrome extractions, which detect phase anomalies or spin flips without directly measuring the protected logical state itself. This preservation of the superposition state during active error monitoring is what allows deep quantum circuits to execute long, multi-tiered computational sequences without collapsing into classical noise.

4.1. Detailed Algorithmic Mechanics: Shor's and Grover's Workflows

To fully understand the computational superiority of quantum frameworks, we must deconstruct the operational workflows of Shor's and Grover's algorithms. Shor's algorithm fundamentally alters cryptography by reducing the problem of prime factorization from exponential time to polynomial time. It achieves this by transforming the factorization task into a period-finding problem on a periodic function, utilizing the Quantum Fourier Transform (QFT) to isolate the period with high probability. This ability to efficiently solve discrete logarithms directly threatens modern security backbones like RSA and Diffie-Hellman, accelerating the necessity for post-quantum cryptographic transitions.

Grover's algorithm, on the other hand, provides a quadratic speedup for entirely unstructured database searches. In a classical framework, finding a specific item out of N unsorted elements requires an average of N/2 evaluations, and a worst-case scenario of N evaluations. Grover's algorithm solves this by utilizing selective phase inversions and diffusion operators, repeatedly rotating the state vector towards the desired target vector within a two-dimensional subspace. This geometric amplification increases the probability amplitude of the correct answer,

requiring only approximately $\pi/4 * \sqrt{N}$ operations. Consequently, it redefines the efficiency metrics for multi-variable optimization problems, brute-force key searches, and complex graph traversal matrices.

5. HARDWARE ARCHITECTURES & COMPARATIVE METRICS

Physical implementation requires strict isolation of quantum states from external macroscopic interference. Currently, two dominant engineering methodologies lead hardware development: Superconducting Transmon loops and Trapped-Ion arrays.

Table 1. Architectural and Performance Metrics of Dominant Hardware Paradigms

Architectural Parameter	Superconducting Qubits	Trapped-Ion Qubits
Physical Mechanism	Artificial Josephson junctions in micro-circuits.	Individual charged ions confined via RF fields.
Operating Temp.	Ultra-low cryogenic levels (~10-20 mK absolute zero).	Room temperature chamber with targeted laser arrays.
Gate Speed	Extremely fast operations (nanosecond range).	Slower gate speeds (microsecond scale).
Coherence Profile	Short operational duration; highly vulnerable to noise.	Significantly longer coherence holding times.
Scalability Track	High scalability using native silicon fabrication methods.	Complex scalability due to spatial laser tracking limits.

5.1. Alternative Hardware Modalities

While superconducting transmon circuits and trapped-ion systems remain the primary paradigms driving corporate hardware investments, alternative technological modalities present unique advantages that could bypass critical scaling bottlenecks. Photonic quantum computing leverages individual particles of light (photons) as qubits, routing them through complex integrated optical networks. The primary benefit of photonic architecture is its natural immunity to atmospheric thermal noise, allowing operations to be conducted entirely at room temperature without expensive dilution refrigerators. Furthermore, because light inherently travels at high velocities, photonic QPUs can seamlessly integrate with existing fiber-optic telecommunications infrastructure, making them ideal candidates for building distributed quantum networks and secure quantum communication channels.

Another promising paradigm is topological quantum computing, which utilizes non-Abelian anyons—quasiparticles that exist in two-dimensional spaces. In a topological system, quantum information is not stored in localized physical properties like particle spin or charge, but is instead woven into the geometric patterns or braids formed by the world-lines of these anyons. Because these braids are topologically protected, local environmental disturbances cannot easily undo or disrupt the global structural arrangements. This gives topological qubits an intrinsic, hardware-level immunity to noise, potentially eliminating the massive software

overhead required by traditional quantum error correction protocols. Though manufacturing stable topological substrates remains a significant solid-state physics challenge, its successful implementation could drastically accelerate the timeline toward true fault-tolerant computing frameworks.

6. PRESENT-ERA CHALLENGES & FUTURE OUTLOOK

The primary engineering bottleneck in contemporary quantum system design remains environmental decoherence. Qubits are highly susceptible to minute thermodynamic and electromagnetic variations, which disrupt fragile probability amplitudes and introduce catastrophic errors during processing cycles. Scaling these platforms to thousands of physical qubits requires exceptionally precise control systems and efficient error correction overlays. Transitioning from noisy NISQ prototypes to fault-tolerant, commercial-grade infrastructures requires sustained optimization across microwave control systems, nanoscale material fabrication, and custom hybrid classical-quantum software compilers.

The practical deployment of quantum computers will also fundamentally reshape the global software ecosystem. Currently, classical software relies on deterministic compilation, where high-level languages are reduced to standard binary logic gates. Quantum software, conversely, requires probabilistic compilers capable of optimizing complex geometric rotations while respecting the strict physical mapping limitations of the underlying hardware layout. Furthermore, the integration of quantum processing units into cloud data centers necessitates the development of sophisticated scheduling algorithms that dynamically distribute complex workloads between CPUs, GPUs, and QPUs. This hybrid infrastructure ensures that tasks are routed to the most efficient processing architecture, maximizing performance outputs across scientific computing networks.

6.1. Real-World Applications: Cryptography and Biochemical Simulation

The real-world impacts of achieving scalable, fault-tolerant quantum ecosystems will manifest prominently across national security infrastructure and molecular engineering. In cryptography, the deployment of Shor's algorithm necessitates an immediate, industry-wide migration toward Post-Quantum Cryptography (PQC). Government agencies and financial institutions are actively standardizing lattice-based cryptographic algorithms, which rely on geometric vector complexities that remain secure against both classical and quantum attacks. Preparing for this cryptographic transition is imperative, as malicious actors currently practice 'harvest now, decrypt later' strategies—intercepting encrypted sensitive data today with the intention of decrypting it once quantum hardware reaches commercial maturity.

In the field of biochemical simulation, quantum processors will revolutionize molecular modeling and drug discovery pipelines. Classical computers fail to accurately simulate complex chemical compounds because calculating the exact quantum mechanical interactions between multiple electrons scales exponentially with the size of the molecule. By mapping the electronic states of a target molecule directly onto highly controllable quantum registers, researchers can utilize algorithms like the Variational Quantum Eigensolver (VQE) to predict precise molecular behaviors and chemical reaction pathways. This capability accelerates the discovery of novel pharmaceuticals, high-efficiency catalyst materials for clean energy

generation, and optimized chemical compounds for industrial manufacturing, effectively condensing decades of traditional laboratory trial-and-error down to mere days of target runtime processing.

7. CONCLUSION

This systematic review highlights the foundational paradigms, algorithmic advantages, and persistent engineering challenges of the quantum computing domain. While physical constraints like decoherence and operational noise restrict current deployment scales, ongoing innovations in error-correcting codes and cryogenic hardware engineering continue to stabilize performance metrics. As development transitions past NISQ-era constraints, hybrid processing environments will reshape computational capabilities, offering transformative advancements across data security, molecular modeling, and global multi-variable optimization matrices.

REFERENCES

[1] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, 10th Anniversary ed., Cambridge, U.K.: Cambridge University Press, 2010.

[2] S. S. Gill, A. Kumar, H. Singh, M. Singh, K. Kaur and R. Buyya, "Quantum Computing: A Taxonomy, Systematic Review and Future Directions," arXiv preprint arXiv:2010.15559, 2020.

[3] J. Preskill, "Quantum Computing in the NISQ Era and Beyond," Quantum, vol. 2, pp. 79, 2018.

[4] R. S. Smith, M. J. Curtis and W. J. Zeng, "A Practical Quantum Instruction Set Architecture," arXiv preprint arXiv:1608.03355, 2016.

[5] D. García-Peral, J. Cruz-Benito and F. J. García-Peñalvo, "Systematic Literature Review of Quantum Computing and Applications," arXiv preprint, 2022.

[6] P. B. Upama, M. J. H. Faruk, M. Nazim et al., "Evolution of Quantum Computing: A Systematic Survey on the Use of Quantum Computing Tools," arXiv preprint arXiv:2204.01856, 2022.

[7] M. Williams, Lecture Notes on Quantum Computing and Quantum Information, University Lecture Series, 2019.

[8] W. Chiang and M. Frank, "Quantum Computing for Computer Architects," Synthesis Lectures on Computer Architecture, Morgan & Claypool Publishers, 2018.

[9] J. Hidary, Quantum Computing: An Applied Approach, Cham, Switzerland: Springer Nature, 2019.

[10] M. Kepe, Quantum Computing Handbook: University Lecture Notes, Department of Computer Science Lecture Series, 2021.

[11] A. Kitaev, "Fault-tolerant quantum computation by anyons," Annals of Physics, vol. 303, no. 1, pp. 2-30, 2003.

[12] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Review, vol. 41, no. 2, pp. 303-332, 1999.

[13] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, 1996, pp. 212-219.

[14] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984, vol. 175, p. 8.

[15] F. Arute et al., "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, pp. 505-510, 2019.

[16] T. D. Ladd et al., "Quantum computers," Nature, vol. 464, pp. 45-53, 2010.

[17] E. Farhi, J. Goldstone and S. Gutmann, "A Quantum Approximate Optimization Algorithm," arXiv preprint arXiv:1411.4028, 2014.

[18] J. R. McClean et al., "The theory of variational quantum eigensolvers and their applications," New Journal of Physics, vol. 18, p. 023023, 2016.

[19] S. Bravyi and A. Kitaev, "Universal quantum computation with ideal Clifford gates and noisy ancilla states," Physical Review A, vol. 71, no. 2, p. 022316, 2005.

[20] A. Peruzzo et al., "A variational eigenvalue solver on a photonic quantum processor," Nature Communications, vol. 5, p. 4213, 2014.