IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, March 2026
Impact Factor: 8.2

Leveraging Quantum Computing to Strengthen Cybersecurity in Banking

Anish Shrimali
Chief Manager, Union Learning Academy- Digital Transformation
Union Bank of India, Mumbai, India

Abstract: *The banking sector remains a high-value target for cyberattacks due to its vital role in managing sensitive financial data and enabling large-scale digital transactions. As digital banking expands, cyber risks increasingly carry systemic implications. In this context, quantum computing represents a fundamental shift in the cybersecurity landscape. Widely used encryption mechanisms such as RSA and elliptic curve cryptography (ECC), which underpin digital banking, payments, and data protection, are vulnerable to future quantum attacks particularly under the "harvest now, decrypt later" (HNDL) threat model, where encrypted financial data collected today may be compromised once quantum computing capabilities mature. This research examines the role of quantum computing in reshaping banking cybersecurity, with emphasis on post-quantum cryptography (PQC), quantum key distribution (QKD), quantum random number generation (QRNG), and quantum machine learning (QML) for fraud detection. Drawing on global and Indian banking practices, regulatory guidance from RBI and SEBI, and policy initiatives such as India's National Quantum Mission, the study proposes a structured roadmap for quantum readiness. The NIST finalization of PQC standards (FIPS 203–205, August 2024) has removed a key barrier to action, enabling banks to begin quantum-safe migration immediately. The study concludes that quantum-safe migration is a strategic imperative requiring phased implementation, architectural modernization, and coordinated regulatory and institutional action.*

Keywords: Quantum Computing, Post-Quantum Cryptography, Quantum Key Distribution, Banking Cybersecurity, Harvest Now Decrypt Later, NIST Standards, Cryptographic Agility, Quantum Random Number Generation, Quantum Machine Learning, Indian Banking, RBI, SEBI

I. INTRODUCTION

1.1 The Quantum Threat to Financial Infrastructure

The global financial system operates on cryptographic foundations established in the 1970s - RSA encryption and later Elliptic Curve Cryptography (ECC) providing security for payment messages, customer authentication, and digital signatures. These systems rely on the computational difficulty of integer factorization (RSA) and the discrete logarithm problem (ECC), both of which quantum computers can solve exponentially faster via Shor's algorithm.

In July 2025, researchers successfully executed Shor's algorithm on an IBM 133-qubit processor to break a 5-bit elliptic curve key, demonstrating that quantum attacks on cryptographic systems are implementable on real hardware. While this represents trivial cryptographic strength, the experiment validates that quantum algorithm execution maintains sufficient coherence to produce cryptographically meaningful results, signalling a trajectory toward full-scale threats.

More immediately threatening is the "harvest now, decrypt later" (HNDL) attack pattern: adversaries collect, and store encrypted data today, anticipating that future quantum computers will enable retroactive decryption of financial records, communications, and authenticated transactions - an attack already in motion globally.

1.2 Scope and Urgency

A June 2025 report from the Global Risk Institute indicates that 27% of quantum experts expect a Cryptographically Relevant Quantum Computer (CRQC) within ten years, with 50% projecting emergence within fifteen years. The U.S.

DOI: 10.48175/IJARSCT-31523

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, March 2026 Impact Factor: 8.2

federal government has set 2035 as the deadline for transitioning national security systems to post-quantum cryptography. NIST completed its eight-year PQC standardization process in August 2024, designating RSA as deprecated after 2030 and disallowed after 2035.

For banking institutions, the transition horizon is simultaneously longer and more compressed—longer due to the complexity of migrating global payment systems and legacy infrastructure, and more compressed because long-lived financial data (mortgages, regulatory records, blockchain histories) creates encryption debt that accrues in quantum time. Early and structured action is therefore both prudent and necessary.

II. PROBLEM STATEMENT AND OBJECTIVES

Indian banking institutions face immediate quantum cybersecurity risks despite current quantum computers being in development stages. The HNDL threat allows malicious actors to collect encrypted banking data today for future quantum decryption, compromising customer information and transaction security. Current RSA and ECC cryptographic systems protecting core banking infrastructure will become vulnerable to quantum attacks, potentially exposing payment systems and inter-bank communications.

Objectives

- To assess how quantum computing threatens existing cybersecurity frameworks in banks.
- To explore practical applications of quantum-safe solutions such as PQC and QKD relevant to banking operations.
- To evaluate quantum computing opportunities for enhanced fraud detection and cybersecurity operations, focusing on practical implementation feasibility for banking environments.

III. METHODOLOGY

The research adopted a practical and analytical approach combining systematic literature review, case analysis, and comparative assessment. Primary data sources included regulatory publications from NIST, RBI, SEBI, MAS, and international cybersecurity agencies. Case examples from JPMorgan Chase, HSBC, DBS, Banco Sabadell, Standard Chartered, and Indian banking institutions were analysed to understand real-world quantum-safe solution deployment.

A comparative evaluation was conducted between current cryptographic practices in banking and emerging post-quantum solutions, focusing on feasibility, scalability, and cost-effectiveness. Market data from authoritative research bodies (Market Research Future, Dimension Market Research, Precedence Research) was synthesized to assess adoption trajectories and inform strategic recommendations.

IV. LITERATURE REVIEW

Recent research indicates that quantum computing could fundamentally alter the cybersecurity landscape of financial institutions. Studies by the Bank for International Settlements emphasize the need for financial institutions to develop quantum□ready security strategies. Similarly, the National Institute of Standards and Technology finalized post□quantum cryptographic standards in 2024 to enable organizations to transition toward quantum□resistant encryption algorithms.

Research by consulting firms such as McKinsey and Deloitte highlights that the financial sector is among the industries most exposed to quantum computing risks. The banking sector must therefore begin planning long□term cybersecurity transformations to protect critical financial infrastructure.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, March 2026
Impact Factor: 8.2

V. RESULTS AND DISCUSSION

5.1 Market Research and Trends

5.1.1 Global Quantum Computing Market

The global quantum computing market demonstrates rapid expansion driven by government R&D investment, private sector competition, and increasing enterprise recognition. Market Research Future projects growth from USD 2.70 billion in 2024 to USD 20.20 billion by 2030, representing a CAGR of 41.8%. The banking and financial services segment dominates quantum computing adoption, representing 26% of market share in 2025, with fraud detection and risk modelling as near-term use cases.

The quantum computing-in-cybersecurity market shows a 32% CAGR, with acceleration sharply post-2030 as quantum threats become operationally relevant. This growth reflects increasing enterprise and government preparedness against HNDL risks, and growing demand for quantum-resistant security infrastructure.

5.1.2 Regional Market Dynamics

Asia-Pacific quantum computing markets demonstrate the highest growth rates, with China, Japan, South Korea, and India as primary innovation centres. India's quantum computing market is projected to expand from USD 89.25 million (2024) to USD 1,235.35 million by 2035 (CAGR: 26.98%), driven by the National Quantum Mission (INR 6,003.65 crore through 2031) and domestic startups such as QNu Labs at IIT Madras Research Park.

North America leads global market share at 40.2%, followed by Europe (28.5%) and Asia-Pacific (22.1%). The QKD market is projected to grow from USD 2,573.8 million (2024) to USD 10,951.8 million by 2032 (CAGR: 23%), with the BFSI segment dominating adoption owing to high-value transaction security needs.

5.1.3 Post-Quantum Cryptography Adoption Market

The PQC migration market is projected to expand from USD 1.9 billion (2025) to USD 12.4 billion by 2035, with three distinct phases: infrastructure assessment and planning (2025–2027); pilot implementations and foundational deployment (2027–2030); and scaled enterprise adoption (2030–2035). Financial services account for 41% of PQC applications, reflecting the sector's critical dependence on cryptographic security and stringent regulatory requirements.

U.S. federal PQC transition costs are projected at USD 7.1 billion (2024 dollars) for 2025–2035, underscoring the scale of required investment. Banks delaying migration face compressed timelines, higher migration risk, and increased operational strain in later phases.

5.1.4 Sector Distribution and Banking Maturity

BFSI leads the quantum cybersecurity market share at 35%, followed by Healthcare (25%), Government (20%), IT and Telecom (15%), and others (5%). Globally, banks such as JPMorgan Chase lead in implementation maturity, with most institutions in pilot or structured experimentation stages. Maturity strongly correlates with R&D spending and technology partnerships, making quantum readiness an emerging competitive differentiator.

5.1.5 India's Quantum Market Growth

India's quantum ecosystem exhibits exponential growth, with cumulative investment rising sharply from ₹1,000 crore (2025) to ₹1.8 lakh crore by 2035. Market value growth significantly outpaces investment, increasing from ₹500 crore (2025) to approximately ₹16.8 lakh crore by 2035, demonstrating investment CAGR of ~78.9% versus market value CAGR of ~111.6%. A pronounced inflection point occurs post-2028, coinciding with ecosystem maturity, regulatory clarity, and early commercialization of quantum applications.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, March 2026 Impact Factor: 8.2

5.2 Present Scenario: Risks and Challenges

5.2.1 Current Cryptographic Landscape in Banking

Contemporary banking security relies fundamentally on RSA and ECC algorithms, forming the foundation of digital signatures, secure communication channels, and payment processing. Large international banks operate independent cryptographic systems across wholesale banking, retail operations, payments, and treasury functions, creating fragmentation that impedes rapid quantum-safe transition.

Current regulatory frameworks (PCI-DSS) mandate encryption but focus on algorithm strength via key length rather than underlying quantum resilience. Existing standards lack specific provisions for quantum threats, creating regulatory gaps that complicate institutional planning and delay proactive migration efforts.

5.2.2 The Harvest Now, Decrypt Later (HNDL) Threat

The HNDL attack pattern allows adversaries to collect, and store encrypted financial communications today, waiting for future quantum decryption capabilities. Banking data retention mandates spanning 5–10+ years compound this vulnerability: sensitive financial data that appears adequately protected today becomes retroactively vulnerable once quantum computers mature. The Federal Reserve Board estimates this risk creates hidden exposure across financial infrastructure, particularly for blockchain applications with immutable transaction histories.

Quantum threat materialization timelines remain uncertain (2030–2060 estimates for breaking RSA-2048), but the delay between current encryption and future decryption vulnerability creates immediate need for proactive cryptographic transition regardless of precise timing.

5.2.3 Vulnerability of Cryptographic Algorithms

RSA security depends on the computational infeasibility of prime factorization; ECC relies on the discrete logarithm problem solvable in polynomial time via Shor's algorithm on quantum hardware. Breaking RSA-2048 is estimated to require approximately 20 million stable qubits with 8-hour coherence, representing dramatic scale-up from current 100–500-qubit systems with significant error rates. Symmetric algorithms (AES-256) face lesser vulnerability via Grover's algorithm (effectively reducing to 128-bit equivalent strength) and remain practically resilient. The critical risk surface is public-key cryptography.

5.2.4 Regulatory and Compliance Drivers

NIST has established binding migration timelines requiring deprecation of quantum-vulnerable algorithms by 2035, with high-risk systems requiring earlier transition. The EU's NIS2 Directive mandates quantum-safe cryptography by 2030 for critical infrastructure; DORA requires European financial institutions to assess quantum computing risks. SEBI has established PQC action plans targeting 2028–2029 operational implementation. PCI-DSS v4.0 (effective March 2025) requires active cryptographic monitoring and documented quantum response plans.

5.2.5 Operational Risk and Infrastructure Complexity

Migration from classical to quantum-safe cryptographic systems introduces substantial operational risks during transition periods. Large banking institutions operate mainframe systems developed decades ago with cryptography embedded directly into system code. Modifying cryptographic implementations within mainframe payment processing systems risks system stability, requires extensive testing, and may require downtime affecting millions of customers.

Hardware security modules (HSMs) require firmware updates to support quantum-safe algorithms. Organizations must manage concurrent operation of classical and quantum-safe HSMs during transition, requiring careful key management. The distributed nature of banking cryptography across multiple business units and jurisdictions further complicates coordinated transition.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, March 2026 Impact Factor: 8.2

5.3 Quantum Computing Technologies: Use Cases and Assessment

5.3.1 Quantum Key Distribution (QKD)

QKD leverages fundamental quantum mechanics principles specifically the disturbance of quantum states upon observation—to securely generate and exchange cryptographic keys. Any eavesdropping attempt immediately reveals intrusion, making undetected interception theoretically impossible.

5.3.1.1 Banking Implementations

The Monetary Authority of Singapore (MAS) conducted a landmark QKD sandbox (2024–2025) with DBS, HSBC, OCBC, and UOB over the National Quantum-Safe Network Plus (NQSN+). HSBC achieved a world-first milestone by securing a £30 million FX transaction using QKD on its trading platform. JPMorgan Chase demonstrated QKD-based networks to secure blockchain-enabled interbank communication channels.

5.3.1.2 Benefits and Limitations

Key benefits include theoretically unbreakable key exchange secured by physical laws, forward secrecy, and production-level readiness for select high-value use cases. Limitations include specialized costly hardware, distance constraints requiring trusted intermediate nodes, lack of authentication capability, and vendor-specific interoperability gaps. Critically, QKD addresses only the key exchange problem and must be combined with PQC for comprehensive quantum-safe security

5.3.2 Post-Quantum Cryptography (PQC)

PQC represents the most practical and immediately deployable approach to quantum-safe banking, operating on classical infrastructure without specialized quantum hardware. NIST finalized three PQC standards in 2024:

ML-KEM (CRYSTALS-Kyber): Module-Lattice Key Encapsulation for secure key exchange resistant to both classical and quantum attacks. Public key size ~2,768 bytes.

ML-DSA (CRYSTALS-Dilithium): Module-Lattice Digital Signature providing authentication, integrity, and non-repudiation. Signature size ~2,420 bytes.

SLH-DSA: Stateless Hash-Based Digital Signature as a conservative alternative based on hash function security assumptions.

Banco Sabadell's successful four-month PQC pilot with Accenture and QuSecure demonstrated integration of quantum-safe cryptography into live banking systems using encryption-agility platforms without infrastructure replacement. Key challenges include increased cryptographic sizes impacting bandwidth and storage, and performance overhead for latency-sensitive systems such as high-frequency trading and real-time payment platforms.

5.3.3 Quantum Random Number Generation (QRNG)

QRNG leverages inherent unpredictability in quantum phenomena to generate truly random numbers, unlike deterministic pseudo-random number generators (PRNGs). Each quantum measurement outcome is independent, ensuring true entropy. In banking, QRNG primarily strengthens cryptographic key generation—strong encryption depends on high-entropy keys, and insufficient randomness increases susceptibility to cryptanalysis.

QNu Labs provides QRNG solutions integrating with standard APIs, HSMs, and existing cryptographic key management frameworks. QRNG is best deployed for security-critical functions where genuine randomness is essential, and serves as a high-impact, low-intrusion entry point into quantum-enhanced security for banks.

5.3.4 Quantum Machine Learning (QML) for Fraud Detection

QML combines quantum computing with machine learning to enhance fraud detection by leveraging quantum superposition to evaluate multiple fraud indicators such as transaction value, location, device attributes, behavioural history, and network relationships simultaneously, enabling deeper pattern recognition beyond classical limits.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, March 2026 Impact Factor: 8.2

Deloitte Italy's hybrid quantum neural network (with Amazon Braket) showed improved fraud detection accuracy versus classical models. HSBC partnered with Quantinuum to explore real-time suspicious activity identification. Current limitations include NISQ-era hardware constraints (high error rates, limited qubit counts), data privacy and regulatory complexity, and limited model interpretability. QML is best positioned as a long-term capability complementing classical systems.

5.3.5 Portfolio Optimization and Risk Analytics

Quantum algorithms (QAOA, VQE) explore combinatorial optimization problems more effectively than classical sequential computation, enabling faster identification of near-optimal asset allocations under complex constraints. JPMorgan Chase (with QC Ware) reported quantum-inspired optimization up to 1,000× faster than traditional methods in selected scenarios. Banco Sabadell explored quantum applications in credit scoring, Standard Chartered investigated trading signal prediction. Hardware maturity remains the primary barrier—current demonstrations apply to simplified problems, not full-scale production portfolios.

5.4 Comparative Analysis of Quantum Technologies

Table 1: Comparative Analysis - Quantum Key Distribution (QKD) vs Post-Quantum Cryptography (PQC)

Dimension	QKD	PQC
Security Basis	Laws of physics (quantum mechanics)	Computational hardness of quantum-resistant math problems
Infrastructure Required	Specialized quantum hardware and secure channels	Software-based; runs on existing IT infrastructure
Deployment Cost	Very high - hardware + network redesign	Moderate - migration and system upgrades
Scalability	Limited; distance and node constraints	Highly scalable across all banking systems
Standards Status	No globally unified standard yet	NIST FIPS 203–205 finalized (2024)
Implementation Timeline	Long-term, phased deployment	Near-term to medium-term deployment feasible
Primary Use Cases	Interbank links, regulator interfaces, high-value transactions	Core banking, payments, customer data, digital signatures
Role in Banking Security	Niche, complementary security layer	Foundational quantum-safe mechanism
Long-Term Viability	Strategic supplement to PQC	Mandatory baseline for quantum-safe banking

Table 2: Quantum Random Number Generation (QRNG) vs Pseudo-Random Number Generation (PRNG)

Dimension	QRNG	PRNG
Source of Randomness	Quantum physical processes	Deterministic algorithms
True Unpredictability	Yes - physics-based, not algorithmic	No - algorithmic approximation
Entropy Quality	Very high (true entropy)	High but finite and predictable

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, March 2026
Impact Factor: 8.2

Dimension	QRNG	PRNG
Resistance to Advanced Attacks	Strong against classical and quantum attacks	Vulnerable if seed/state is compromised
Infrastructure Requirement	Specialized hardware or cloud service	Software-only - low overhead
Cost	High - hardware or subscription fees	Low
Performance Throughput	Moderate	High
Best Use Cases	High-value cryptographic key generation, HSMs	General-purpose cryptographic operations

Table 3: Classical Machine Learning vs Quantum Machine Learning - Fraud Detection Context

Dimension	Classical ML	Quantum ML (QML)
Data Processing	Sequential / parallel (classical)	Parallel evaluation via quantum superposition
Fraud Pattern Detection	Known and statistical patterns	Ability to detect subtle, non-linear patterns
Accuracy	Mature and reliable	Early-stage, promising but experimental
False Positive Rate	Moderate	Potentially lower (richer feature correlation)
Technology Maturity	High — production-ready	Low–medium — NISQ stage
Explainability	High	Limited and still evolving
Regulatory Acceptance	High	Cautious / exploratory
Deployment Scope	Enterprise-wide primary system	Pilot / decision-support role
Role in Banking Today	Primary fraud detection engine	Complementary, future-enhancing tool

Table 4: Classical Optimization vs Quantum Optimization - Banking Context

Dimension	Classical Optimization	Quantum Optimization
Computational Approach	Sequential / parallel classical computation	Probabilistic, quantum-enhanced search
High-Dimensional Problems	Limited by time and compute resources	Potentially superior for combinatorial problems
Speed	Slower for complex, constraint-heavy portfolios	Faster convergence in hybrid experimental cases
Algorithm Examples	Mean-variance, Monte Carlo simulation	QAOA, VQE, quantum-inspired heuristics

DOI: 10.48175/IJARSCT-31523

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, March 2026 Impact Factor: 8.2

Dimension	Classical Optimization	Quantum Optimization
Maturity Level	Fully production-ready	Experimental / early-stage
Explainability	High	Limited, still evolving
Validation Effort	Established back-testing processes	Extensive back-testing required
Current Role in Banks	Primary optimization and risk engine	Research / decision-support tool
Long-Term Potential	Incremental improvement	Transformational (as hardware matures)

5.5 Global and Indian Bank Adoption

5.5.1 Global Banking Implementations

JPMorgan Chase pioneered quantum-safe networking by demonstrating a 10 Gbps QKD-secured IPsec tunnel between two datacentres over a 46 km metropolitan fibre link, combining QKD at the network layer with PQC at the application layer—setting an industry model for layered quantum defences in finance.

HSBC became the first bank on BT/Toshiba's UK QKD metro network in July 2023, linking its Canary Wharf HQ to a data centre via a 62 km QKD-encrypted channel and securing high-value FX transactions (~€30 million). It separately established a Quantum Centre of Excellence in Singapore. Banco Sabadell completed a four-month PQC pilot with Accenture and QuSecure (late 2024), producing a detailed roadmap for migrating to NIST-standard quantum-resistant algorithms. Standard Chartered collaborated with Capgemini on a PQC Proof-of-Concept assessing ML-DSA, SLH-DSA, and Falcon schemes against RSA for banking workloads.

Intesa Sanpaolo (Italy) pioneered Fully Homomorphic Encryption (FHE) with IBM's HELayers platform, enabling computations on encrypted customer transaction data without exposing underlying data. Crédit Mutuel Alliance Fédérale joined IBM's Quantum Network as the first French bank, accessing 433-qubit systems for fraud detection and risk modelling. BBVA and Santander co-founded the Quantum Safe Financial Forum (QSFF) under Europol, coordinating global PQC migration across international banks and regulators.

5.5.2 Indian Banking Adoption

HDFC Bank leads among Indian banks with a strategic investment in QNu Labs (announced September 2025), obtaining full-stack quantum-safe cybersecurity platform coverage via QShield with physics-based key distribution. ICICI Bank follows with above-average preparedness (3.0/5.0), while Kotak Mahindra, SBI, and Axis Bank cluster around the sector average (2.5/5.0). Public sector banks score lowest (1.5/5.0), reflecting legacy systems and resource constraints.

The Reserve Bank of India Innovation Hub has explicitly recommended that banks embark on proactive transition to quantum-resistant algorithms, including crypto asset inventorying and phased PQC upgrades for payment systems, internet banking, and data centres. SEBI has drawn up an action plan for quantum-safe securities markets by 2028–2029. NPCI is reportedly developing quantum-resistant cryptography protocols for UPI and real-time payment rails to protect billions of daily payments against HNDL threats.

5.5.3 Indian Banking Readiness Assessment

Post-quantum cryptography readiness in India is highly uneven. Private banks demonstrate the highest overall readiness (scoring above 4.0/5.0 across all dimensions). Payment networks show balanced readiness (70–80%). Fintechs demonstrate high quantum awareness but lower regulatory compliance. Public sector banks show moderate readiness (50–75%) constrained by legacy infrastructure. NBFCs are least prepared (35–60%), requiring targeted policy support and phased capability-building to avoid systemic vulnerabilities.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, March 2026 Impact Factor: 8.2

India's PQC adoption trajectory is regulation-led and non-linear: from pilot research (3% adoption in 2025) progressing toward full-scale adoption (100% by 2035), with a critical inflection point around 2028–2029 aligned with SEBI regulatory targets. By 2035, approximately 2,500 institutions are expected to have completed transition, indicating that post-quantum cryptography becomes a system-wide requirement rather than a competitive differentiator.

5.6 Implementation Strategies

Banks that adopt a portfolio approach combining multiple quantum technologies based on risk exposure and institutional capacity will achieve the best quantum-safe outcomes. The following strategic framework is proposed based on global best practices and Indian banking context:

5.6.1 Comprehensive Cryptographic Inventory and Risk Assessment

Conduct automated discovery and manual categorization of all cryptographic usage by algorithm type, key length, data sensitivity, and retention period. Risk scoring should evaluate each system based on quantum vulnerability, business criticality, regulatory sensitivity, and HNDL exposure timeline. This inventory forms the foundation for all subsequent migration planning.

5.6.2 Hybrid Cryptography Transition

Simultaneous deployment of classical algorithms (RSA, ECC) alongside quantum-safe algorithms (ML-KEM, ML-DSA) ensures security remains intact if either method is compromised, maintaining backward compatibility during phased migration. This dual-layer approach protects long-lived financial data while preserving compatibility with legacy infrastructure and external counterparties.

5.6.3 Cryptographic Agility Architecture

Abstraction of cryptography through centralized key management systems, standardized APIs, and policy-driven controls enables rapid algorithm replacement without system redesign. This significantly reduces long-term regulatory response time and technical debt, allowing banks to adapt as standards and threat landscapes evolve.

5.6.4 Risk-Based Prioritization

Focus quantum-safe upgrades on payments, core banking, customer data, and interbank systems first. Systems managing highly sensitive, long-retention data most vulnerable to HNDL attacks warrant earliest transition. Lower-risk or isolated systems can follow on extended timelines, optimizing resource allocation and operational impact.

5.6.5 Quantum-Safe Network Infrastructure

Deploy dedicated communication channels secured by PQC or selective QKD for high-value interbank and regulator communications. Models range from private fibre-based networks connecting data centres to shared national quantum-safe networks (e.g., India's National Quantum Mission infrastructure), which reduce per-institution investment.

5.6.6 Hardware Security Module (HSM) Modernization

Upgrade to quantum-ready HSMs supporting both classical and post-quantum algorithms with centralized key management, tamper-resistant hardware, and integration with enterprise key management platforms. Cloud-based HSM services offer flexible adoption models. HSM modernization anchors quantum-safe security at the core of banking cryptographic infrastructure.

5.7 Implementation Challenges and Mitigation Strategies

Eight primary implementation challenges are identified along with corresponding mitigation strategies:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, March 2026
Impact Factor: 8.2

5.7.1 Legacy System Integration

- Challenge: Mainframe systems with cryptography embedded in system code resist modification.
- Mitigation: Implement cryptographic abstraction layers and HSM-based centralized services, enabling algorithm changes without modifying underlying system code. Gradual system modernization prioritizes replacement of oldest systems.

5.7.2 Interoperability

- Challenge: Quantum-safe transition requires coordinated implementation across clearing houses, settlement systems, correspondent banks, and payment networks with varying timelines.
- Mitigation: Hybrid cryptographic approaches and industry consortia coordination (BCBS, FSB, QSFF) establish common transition standards and timelines.

5.7.3 Performance Overhead

- Challenge: Post-quantum algorithms impose computational overhead , larger cryptographic material and more complex key generation that impacts latency-sensitive systems.
- Mitigation: Hardware acceleration via specialized cryptographic processors, gradual hybrid transition, and algorithm parameter optimization for high-frequency trading and real-time settlement platforms.

5.7.4 Workforce Skill Gaps

- Challenge: Post-quantum cryptography requires specialized domain knowledge such as lattice mathematics, learning with errors problems beyond traditional cryptographic expertise.
- Mitigation: University partnerships, vendor training programs (IBM, Microsoft, Quantinuum), role rotation programs, cloud-based quantum-safe services, and targeted recruitment from academic institutions.

5.7.5 Regulatory Ambiguity

- Challenge: Evolving regulatory frameworks across jurisdictions create potentially conflicting compliance requirements. Mitigation: Proactive regulatory engagement, participation in standards working groups, comprehensive transition plan documentation, and automated compliance reporting systems.

5.7.6 Vendor Ecosystem Maturity

- Challenge: PQC represents an emerging market with incomplete vendor ecosystem and single-vendor dependency risks. Mitigation: Open-source cryptographic libraries (liboqs), multi-vendor evaluation strategies, and industry consortium participation to develop interoperable quantum-safe solutions.

5.7.7 Cost and Capital Requirements

- Challenge: Quantum-safe infrastructure modernization requires substantial capital across multiple infrastructure layers. Mitigation: Phased implementation across budgetary cycles, cloud-based operational expense models, and cost-sharing collaborative implementations to reduce per-institution investment.

5.7.8 Legacy Data Protection

- Challenge: Historical data encrypted with classical algorithms remains vulnerable to HNDL attacks. Re-encryption is logistically complex.
- Mitigation: Prioritized protection of newly generated data with quantum-safe cryptography, targeted re-encryption of highest-value legacy data, and cryptographic key destruction for data no longer required under retention policy.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, March 2026
Impact Factor: 8.2

5.8 Recommendations

Based on research findings, thirteen prioritized recommendations are presented for banking institutions and Indian regulators:

- **Establish Quantum Risk Visibility:** Conduct comprehensive cryptographic inventory and risk assessment to quantify quantum threat exposure, prioritizing by data sensitivity, retention requirements, and business criticality.
- **Launch Targeted Quantum-Safe Pilots:** Allocate dedicated resources to controlled pilot programs testing PQC, hybrid encryption, and cryptographic agility in selected systems before large-scale deployment.
- **Build Strategic Quantum Partnerships:** Evaluate vendor partnerships such as QNu Labs for Indian quantum-safe solutions to support indigenous quantum-resilient infrastructure development.
- **Position Quantum Cybersecurity as a Strategic Risk:** Treat quantum-related cyber risk as a long-term systemic risk with explicit Board and Risk Committee oversight and clear senior management ownership.
- **Adopt Post-Quantum Cryptography as Core Défense:** Deploy NIST-standardized algorithms (ML-KEM, ML-DSA, SLH-DSA) as the foundation of quantum-safe security for systems handling sensitive and long-lived data.
- **Use Hybrid Cryptography for Smooth Transition:** Combine classical and post-quantum algorithms to ensure continuous protection, backward compatibility, and phased migration without disrupting critical banking operations.
- **Embed Cryptographic Agility in IT Architecture:** Build rapid algorithm-switching capability through centralized key management and modular cryptographic frameworks, reducing long-term technology and compliance risk.
- **Prioritize High-Risk Systems First:** Apply a risk-based approach focusing initial quantum-safe upgrades on payments, core banking, customer data, and interbank systems for maximum security impact.
- **Deploy Advanced Quantum Controls Selectively:** Use QKD and QRNG only for high-value, high-risk communication channels as complements to PQC, not as standalone solutions.
- **Modernize Hardware Security Modules:** Upgrade to quantum-ready HSMs for secure key management, regulatory compliance, and long-term cryptographic resilience.
- **Pilot Quantum Machine Learning Cautiously:** Explore QML through controlled pilots and decision-support roles while maintaining classical ML as the primary fraud detection mechanism.
- **Strengthen Skills and Ecosystem Partnerships:** Invest in quantum-relevant workforce skills, establish centres of excellence, and collaborate with technology providers, fintechs, and academic institutions.
- **Align Early with Regulatory Expectations:** Proactive alignment with RBI, SEBI, and global regulatory timelines (NIST 2035 deadline; SEBI 2028–2029 targets) enables orderly, cost-effective quantum-safe transition.

VI. CONCLUSION

Quantum computing presents a structural shift in the cybersecurity landscape of banking- one that requires deliberate action today despite uncertainty around precise threat timelines. The rapid growth of the global quantum cybersecurity market (CAGR: 32%), led by the BFSI sector, reflects broad recognition that existing cryptographic foundations will not remain resilient in the long term. The HNDL threat has already transformed quantum risk from a future concern into a present-day strategic issue, particularly for financial data with long confidentiality requirements.

The NIST PQC standardization (FIPS 203–205, August 2024) has removed a key barrier to action, enabling banks to begin quantum-safe migration immediately without waiting for quantum hardware maturity. Global implementation experience from JPMorgan Chase, HSBC, DBS, OCBC, UOB, Banco Sabadell, and Standard Chartered demonstrates

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, March 2026 Impact Factor: 8.2

that phased, well-governed quantum-safe transitions are feasible in complex banking environments. While QKD and QML offer additional security and analytical advantages, PQC remains the foundational enterprise-wide control.

For Indian banking, quantum readiness is highly uneven and regulation-led. India's National Quantum Mission, SEBI's 2028–2029 targets, and RBI's proactive recommendations establish a clear trajectory, but progress depends critically on modernizing legacy systems, building skilled talent, and aligning regulatory frameworks across the banking ecosystem. Private banks lead, but public sector banks and NBFCs require targeted policy support to avoid systemic vulnerabilities.

The quantum-safe transition is neither an immediate crisis nor a distant abstraction; it is a multi-year strategic transformation that aligns technical readiness, regulatory mandates, and competitive strategy. Banks that treat quantum safety as a strategic opportunity rather than a compliance obligation will gain resilience, cost efficiency, and early access to quantum-enabled capabilities in fraud detection and risk management. Those that delay risk compressed timelines, higher costs, and operational disruption, repeating the costly lessons of past delayed technology transitions.

REFERENCES

[1] Bank for International Settlements. (2024). Quantum-readiness for the financial sector: A strategic framework. BIS Papers No. 158.

[2] Cryptomathic. (2025, August). PQC migration challenges and compliance risks for financial institutions. Retrieved from https://www.cryptomathic.com/

[3] Deloitte. (2024, July). Quantum machine learning for digital payments fraud detection. AWS Blog.

[4] Dimension Market Research. (2025, July). Quantum computing in cybersecurity market report. Retrieved from https://dimensionmarketresearch.com/

[5] Encryption Consulting. (2025, October). Preparing for the quantum shift in the finance industry. Retrieved from https://www.encryptionconsulting.com/

[6] European Commission. (2024). Network and Information Security Directive 2 (NIS2) implementation guidance. Brussels: EU Publications.

[7] Federal Reserve Board. (2025, September). Harvest now, decrypt later: Examining post-quantum cryptography and data privacy risks. FEDS Discussion Paper Series.

[8] Fortanix. (2024, December). Achieving cryptographic agility: Best practices and implementation strategies. Retrieved from https://www.fortanix.com/

[9] IBM Quantum. (2024). Qiskit runtime: Cloud-based quantum execution service. Retrieved from https://www.ibm.com/quantum/qiskit/

[10] Knowledge Sourcing Institute. (2025, November). Quantum computing market size and forecast 2025–2030. Retrieved from https://www.knowledge-sourcing.com/

[11] McKinsey & Company. (2025, November). The quantum leap in banking: Redefining financial performance. Retrieved from https://www.mckinsey.com/

[12] Monetary Authority of Singapore. (2025, September). Quantum key distribution sandbox technical report. MAS Financial Stability Report.

[13] National Institute of Standards and Technology. (2024, August). Post-quantum cryptography standards: FIPS 203, FIPS 204, FIPS 205. Washington, DC: U.S. Department of Commerce.

[14] Open Quantum Safe. (2025). liboqs: Post-quantum cryptography library. Retrieved from https://openquantumsafe.org/

[15] Palo Alto Networks. (2024, December). The quantum computing threat: Understanding harvest now, decrypt later attacks. Security Brief.

[16] Precedence Research. (2025, May). Quantum computing market size and forecast 2025–2034. Retrieved from https://www.precedenceresearch.com/

[17] QNu Labs. (2024, December). Quantum cybersecurity for banking and finance. Industry Whitepaper.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, March 2026 Impact Factor: 8.2

[18] Reserve Bank of India Innovation Hub. (2024, August). Securing the Indian banking sector from quantum attacks. RBIH Report.
[19] Securities and Exchange Board of India. (2025, October). Quantum-safe computing action plan for capital markets. SEBI Circular.
[20] Singapore Ministry of Communication and Information. (2025). National Quantum-Safe Network Plus (NQSN+) infrastructure initiative. Singapore Quantum Strategy.
[21] SpinQ Technology. (2025, October). Quantum computing industry trends 2025: Breakthrough milestones and commercial transition. Retrieved from https://www.spinquanta.com/
[22] Techni Informed. (2025, March). JPMorgan and HSBC lead global banks in quantum technology race. Retrieved from https://techinformed.com/
[23] The Quantum Insider. (2024, December). Banco Sabadell collaborates with Accenture and QuSecure to implement post-quantum cryptography. Retrieved from https://thequantuminsider.com/
[24] Thales Group. (2022, August). Hardware security modules: Quantum-ready cryptographic platforms. Retrieved from https://cpl.thalesgroup.com/
[25] World Economic Forum. (2025, July). Banking in the quantum era: Three strategic shifts in financial services. Accenture Report.
[26] Wortze, R., & Patterson, T. (2024). Barriers to implementing quantum-resistant encryption in financial institutions. International Journal of Cryptographic Research, 8(2), 45–67.
[27] Zentner, A. (2025). Quantum computing and cybersecurity in accounting and auditing. International Journal of Professional Accounting and Auditing, 12(1), 89–114.