iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** XI **Month of publication:** November 2025

DOI: https://doi.org/10.22214/ijraset.2025.75045

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XI Nov 2025- Available at www.ijraset.com

Post Quantum Cryptography Review: Quantum-Safe Evolution, Applications and Global Market Surge

Vivek Gujar
Chief Strategy Officer, Indoai Technologies P Ltd

Abstract: ***In the wake of accelerating quantum computing threats, Post-Quantum Cryptography (PQC) emerges as a vital shield for global data security, that will poised to revolutionize industries by 2030. This review article traces cryptography's evolution from ancient ciphers to NIST's 2025 standards, detailing quantum-resistant algorithms like ML-KEM and ML-DSA that counter Shor's algorithm vulnerabilities. Potential real-world applications in finance, healthcare, cloud computing and beyond, it highlights PQC's role in safeguarding sensitive transactions, patient records and IoT networks amid projections of Q-Day as early as 2029. With the PQC market surging from $0.42 billion in 2025 to potentially $29.95 billion by 2034, driven by regulatory mandates and innovation, the paper underscores India's GCCs as quantum-ready hubs unlocking trillions in value through strategic adoption. Also,as data Centres are projected to grow to $100B by 2027, needs immediate migration to avert catastrophic breaches, this article equips stakeholders to strategise the quantum era's challenges and opportunities.***

Keywords: Post-Quantum Cryptography, PQC, Quantum-Resistant Algorithms, NIST Standards, Cloud Security, Healthcare Data Protection.

I. INTRODUCTION

Quantum computers are designed to outperform standard computers by running quantum algorithms. Areas in which quantum algorithms can be applied include cryptography, search and optimisation, simulation of quantum systems and solving large systems of linear equations[1]. Quantum computing, utilizing quantum mechanics, promises to outperform classical computers for specific tasks[2]. Quantum computers can solve complex problems much faster than regular computers, using ideas like Shor's algorithm to crack common encryption like RSA[3]. This puts sensitive data at risk. A new study from Google Quantum AI estimates that breaking RSA-2048 encryption could be achieved in under a week using fewer than one million noisy qubits[15]. Post Quantum Cryptography (PQC) provides algorithms that resist these quantum threats, keeping information safe. The evolution of data security has progressed through several stages, intertwining with advancements in information security and cryptography. Initially, security of information was focused on physical safeguards and simple substitution ciphers as early as 1900 BC in ancient Egypt with non-standard hieroglyphs, here one of the first implementations of cryptography was found in the use of non-standard hieroglyphs carved into the wall of a tomb[4]. By the medieval period, polyalphabetic ciphers like Vigenère[5] emerged in 1586, enhancing message protection. The 20th century was about conventional cryptography advance with mechanical devices such as the Enigma machine during Worls War II (1918-1940s), invented by German engineer Arthur Scherbius, used for the encryption and decryption of messages and communications[6]; followed by digital standards like DES in 1975, in 1976, Diffie and Hellman proposed the public key cryptosystem, which solved the problem of key distribution[7], and RSA in 1977[8].

The quantum era began with the proposal of Quantum Key Distribution (QKD) protocols like BB84 in 1984, proposed by Charles Bennett and Gilles Brassard in 1984[9] but the real game changer was Shor's algorithm in 1994, which exposed vulnerabilities in conventional systems[10]. The author [11] demonstrated vulnerabilities in RSA-2048 and ECC-256 under Shor’s algorithm, emphasizing the necessity for quantum-resistant cryptography. This led to Post Quantum Cryptography PQC, with NIST initiating its standardization in 2016 and finalizing algorithms in 2024 to ensure future-proof security[12].

By 2025, the U.S. National Institute of Standards and Technology (NIST)[16] has released key PQC standards, including ML-KEM for key sharing and ML-DSA for signatures[13]. These help businesses move to safer systems. The focus here is on how PQC applies to real-world uses and drives market changes, especially in cloud data handling where long-term security is crucial. Without PQC, companies could lose trust and face big risks by 2030. Without robust quantum-resistant cryptographic strategies, nations risk losing control over critical health infrastructure[14].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XI Nov 2025- Available at www.ijraset.com

II. TECHNICAL DETAILS[17]

Post-quantum encryption algorithms must be based on math problems that would be difficult for both conventional and quantum computers to solve[18]. PQC methods are used because Lattice-based cryptography, code-based cryptography and hash-based cryptography are some of the math problems that are thought to be too hard for quantum computers to solve[19], unlike old methods vulnerable to quantum speedups. NIST selected algorithms after testing many since 2016.

A. Key ones include

- ML-KEM

Core uses**:**

- Key Exchange: Establishing a shared, secret key between two parties communicating [20] in a way that resists attacks from future quantum computers.
- Secure Messaging: Establishing quantum-resistant encryption keys for messaging applications to protect against both classical and quantum attacks[21 https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.203.pdf].
- VPNs and Secure Tunnels[22][23]: Creating secure communication channels by using ML-KEM to establish the initial session keys.
- Cloud Storage Encryption[25][24]**:** Protecting the encryption keys that secure stored data in cloud services.

Smart home systems could rely on the ML-KEM to establish secure encryption keys for device communication[naggy]

- ML-DSA[26][62]: For signing documents, efficient for daily use.

Core Uses

- Electronic Document Signing: Verifying the authenticity of digital documents.
- Secure Software Distribution[27]: Confirming the origin and integrity of software packages to protect against tampering.
- Financial Transactions: Securing electronic fund transfers and digital contracts.
- Dual-Usage Certificates**:** Research has explored protocols for using a single certificate to include public keys for both a KEM and a DSA, allowing for flexible cryptographic schemes[28]

- SLH-DSA[29]: It is used for digital certificates, electronic voting and authenticating [30].

III. APPLICATIONS

PQC is moving from theory to practice in 2025, protecting data across industries. Its uses focus on securing communications, storage and devices against future quantum threats. Let's take a closer look at key areas:

A. Cloud Computing and Data Storage

Cloud services like Google Cloud[31] use PQC for encrypted storage and transfers. AWS provides PQC support for its Transfer Family service[32] to securely move data to and from its cloud use NIST algorithms to S3 buckets, keeping data safe even if stolen now for later cracking. Experimental study[33] demonstrates that quantum-safe algorithms can be integrated into core communication protocols like TLS, IPsec and gRPC with manageable overhead. In Kubernetes[45], PQC secures container communications. This protects big data sets in multi-user clouds.

B. Finance

Banks handle sensitive transactions, so PQC is key. It secures online banking and payments against quantum attacks[34]. JPMorgan touts PQC breakthrough for digital signatures[35]. Executive Order of January 2025 Promotes adoption of PQC technologies, accelerating transition of federal cryptographic systems to PQC use and By end of 2025, financial services lead adoption for secure communications[36], ledgers and trades[37][38]. Transitioning to PQC will allow banks to secure sensitive customer data, protect transaction integrity, and ensure long- term privacy[46].

C. Healthcare

PQC is a critical innovation for securing telemedicine patient data against emerging quantum computing threats[39]**.** Patient data must stay private, utilization of post-quantum cryptography and quantum-resistant algorithms is increasingly crucial in order to

protect sensitive patient data[40]. PQC encrypts medical records and telehealth links. Hospitals use it to meet regulations like HIPAA, protecting against data breaches[41]. Thus, By integrating PQC with quantum key distribution (QKD) and privacy-preserving mechanisms, data confidentiality and immutability for patient records in a post-quantum era are ensured[42]. In 2025, assessments show healthcare needs PQC for long-term record safety.

D. Government and Defense

Federal agencies are being directed to begin incorporating post-quantum[43]. Governments adopt PQC for classified info. NSM-10 (National Security Memorandum 10), A U.S. government mandate establishes a clear deadline for the complete migration to PQC by 2035. Tools like buyer's guides[44] help agencies pick PQC products, as the US government prepares for a future when quantum computers could crack today's encryption systems[45].

E. Internet of Things (IoT) and Networks

NIST's newly finalized lightweight cryptography standard provides a defense from cyberattacks for even the smallest of networked electronic devices[47]. Smart devices need lightweight PQC. One study [48]suggest optimized algorithms for PQC solutions that are lightweight and suitable for deployment in edge computing nodes and Internet of Things devices, considering the resource-constrained IoT situations, thus, its used in IoT for secure updates and in networks for quantum-safe connections. Web browsers and sites add PQC to TLS for safer browsing to provide long-term data confidentiality[49]

F. Blockchain and Emerging Tech

PQC strengthens blockchain against quantum hacks, aiding crypto and supply chains[50]. Solana developers have launched an optional quantum-resistant vault designed to safeguard user funds from future threats posed by quantum computing[51]. It pairs with AI for secure data analysis. The deployment of quantum advancements in blockchain brings about an improved functional capacity and strengthened protection against threats so blockchain becomes a sustainable decentralized platform in the post-quantum realm[52]. Meta (Facebook) wrote about their internal adoption: they have started using hybrid post-quantum TLS in their data centers to secure traffic between data center systems that might be recorded and later attacked[53]. These applications show PQC's wide reach, with hybrids easing rollout but adding some speed costs.

IV. MARKET IMPACT AND GROWTH

The PQC market is mainly driven by the increasing need to safeguard sensitive data from the rising dangers posed by quantum computing[54]. PQC is reshaping markets, especially data clouds, by making security a selling point. market is reshaping industries by mitigating quantum threats, meeting regulatory mandates, and securing cloud and IoT[55]. The market starts at $0.42 billion in 2025 and could hit $2.84 billion by 2030, growing at 46% yearly. Some forecasts see it reaching $29.95 billion by 2034.

A. Impact on India's GCC Business

Cloud is undergoing a seismic shift in the global capability centers ecosystem**[**56**].** India's Global Capability Centers (GCCs), numbering over 1,900[57] and contributing nearly USD 46 billion to the economy in FY2024[58], stand to be profoundly affected by PQC adoption as they evolve into quantum-ready innovation hubs.

The India National Quantum Mission (INR 6,003.65 crore, or USD 740M) has committed to 2030 to seed quantum R&D hubs and an explicit national signal to domestic GCCs to participate[59], GCCs are poised to lead in developing PQC solutions for sectors like finance, pharmaceuticals, and cybersecurity, where quantum threats could otherwise expose sensitive offshore data(see table [59] below). This shift offers opportunities for revenue growth through PQC pilots, hybrid algorithm testing, and talent upskilling programs, potentially unlocking trillions in value via optimized operations and compliance advantages; however, challenges like talent shortages and migration costs require strategic partnerships with academia and government to ensure GCCs remain competitive in the global data security race.

Table[59]

Industry	Quantum Use Case	Role for GCCs	Economic Advantage
BFSI	Portfolio optimisation, fraud detection	Build hybrid quantum-classical algorithms, run pilots	Better risk-adjusted returns; lower fraud losses.

Pharma	Molecular simulation, lead discovery	Integrate quantum simulations with cheminformatics.	Shorter R&D cycles; lower drug discovery cost.
Supply Chain	Route & inventory optimisation	Prototype quantum-enhanced optimisers	Reduced logistics cost; improved SLAs.
Cybersecurity	Post-quantum cryptography	Develop migration plans and PQC testing labs.	Future-proofed data protection; regulatory compliance.

B. Adopting Companies[60]

Leaders include AWS, Google Cloud, and IBM for cloud PQC. Specialists like PQShield, QuSecure, and Thales offer tools. NXP and Palo Alto Networks focus on hardware and networks. Cloud-natives like Zscaler claim "quantum-safe" to win clients. Early movers in finance gain market share.

Company	Technology / Focus Area	Use Case / Go-to-Market Strategy
AWS	Cloud PQC	Providing quantum-safe cryptography services and tools within their cloud infrastructure.
Google Cloud	Cloud PQC	Integrating post-quantum algorithms into cloud services and client libraries.
IBM	Cloud PQC	Offering quantum-safe security solutions and expertise through their cloud and consulting divisions.
PQShield	PQC Tools & Solutions	Specializing in quantum-safe cryptographic solutions for software, hardware, and communications.
QuSecure	PQC Tools & Solutions	Providing orchestration platforms and tools to facilitate the transition to post-quantum cryptography.
Thales	PQC Tools & Solutions	Offering general PQC tools and solutions, often with a focus on high-assurance and government applications.
NXP	Hardware	Developing and manufacturing secure hardware elements (e.g., chips, HSMs) with PQC capabilities.
Palo Alto Networks	Networks	Integrating quantum-resistant security principles into network security firewalls and platforms.
Zscaler	Cloud-Native Security	Marketing "quantum-safe" as a feature to win clients by securing internet and private access.
Early Movers in Finance	PQC Implementation	Gaining market share by being first to adopt PQC, building trust and a security advantage.
Seventhsense	Face-Based PQC & Privacy-Preserving Identity	Delivering SenseCrypt platform for secure eID and PKI using NIST-compliant PQC (ML-KEM, ML-DSA) with facial verification; targets governments, enterprises, and individuals for fraud prevention and passwordless access via API-based deployment in centralized/decentralized systems.

Only 5% of top sites use PQC in 2025(see below section), showing room for growth. Claims like "Your data is safe with us" build trust, but need audits to avoid issues.

C. PQC Adoption Statistics [61]

The report highlights a significant gap between quantum computing advancements and organizational preparedness. Q-Day, when quantum computers could break public-key cryptography, is projected as early as 2029. However, only 5% of CISOs consider post-quantum cryptography (PQC) a high priority, per the ISACA poll. Global PQC readiness stands at 57%, heavily influenced by browser support.

Among the top 1 million websites, hybrid PQC key exchange adoption is low at 8.6%, with 25% lacking TLS 1.3 and 16% without quantum-resistant symmetric ciphers. Adoption varies by rank: 42% for the top 100 sites, dropping to 26% for ranks 100–200, 21.9% average for top 1,000, 13.9% for top 10,000, and 8.4% for top 100,000. This indicates hesitancy, especially beyond high-traffic domains.

Security-sensitive sectors lag notably. Banking websites show only 3% PQC support, the lowest even within finance. Healthcare and government sites also exhibit low uptake, underscoring vulnerabilities in critical areas handling sensitive data.

Geographically, top-level domains (TLDs) from Australia (.au), Canada (.ca), and the UK (.uk) lead in adoption rates and volume. By company headquarters, the United States dominates, followed by the UK, Canada, and Australia, reflecting concentrated efforts in these regions.

Websites supporting PQC demonstrate superior TLS configurations: fewer cipher suites, modern protocols, and disabled outdated ones like SSLv3 and TLSv1.0. Non-PQC sites often retain weak, obsolete options, making PQC a marker of overall cryptographic health.

On the client side, browser readiness varies: Chrome leads with 93% PQC-ready requests, Firefox at 85% (despite 2% market share), while Safari's zero support drags down global figures. Overall, while TLS 1.3 is widespread, PQC rollout remains sluggish. For long-term data confidentiality, immediate deployment is urged to mitigate future quantum risks

Table 1: General Insights on Quantum Risks and Priorities

Metric	Value/Description	Notes/Source
Estimated Q-Day Arrival	As early as 2029	Date when quantum computers can break public key cryptography.
CISOs Viewing PQC as High Business Priority	5%	From ISACA Pulse of Quantum Computing poll.
Overall PQC Readiness (Global, Influenced by Browsers)	57%	Reduced due to Safari's lack of support.

Table 2: PQC Adoption Among Top Websites by Rank

Website Rank Category	PQC Support Percentage	Additional Notes
Top 100	42%	Highest adoption among popular sites.
Ranks 100–200	26%	Noticeable drop from top 100.
Top 1,000 (Avg)	21.90%	Reflects broader trends in high-traffic sites.
Top 10,000	13.90%	Further decline in adoption.
Top 100,000	8.40%	Low overall uptake.
Top 1 Million (Overall)	8.60%	For hybrid PQC key exchange mechanisms; 25% lack TLS 1.3 support; 16% fail quantum-resistant symmetric ciphers.

Table 3: Sector-Specific PQC Adoption

Sector	PQC Support Percentage	Notes
Banking	3%	Among the lowest adopters, even within Financials sector (referenced in Figure 1 of the report).
Healthcare	Low (not quantified)	Lagging in adoption, security-sensitive sector.
Govt	Low (not quantified)	Lagging in adoption, security-sensitive sector.

Table 4: Geographical PQC Adoption

Category	Leading Regions/Countries	Notes
By Top-Level Domain (TLD)	Australia (.au), Canada (.ca), UK	Leading in adoption rate and volume.
By Company Headquarters	United States (global leader), followed by UK, Canada, Aus	US stands out globally.

Table 5: Website Configuration Insights

Aspect	Description for PQC-Supporting Sites	Description for Non-PQC Sites	Notes
TLS Configurations	Stronger overall; fewer and more modern cipher suites; disable outdated protocols (e.g., SSLv3, TLSv1.0).	Commonly support weak and obsolete protocols; offer more cipher suites (less hardening).	PQC support acts as a proxy for broader cryptographic hygiene.

Table 6: Client-Side (Browser) PQC Readiness

Browser	PQC-Ready Traffic(%)	Share of Total Requests	Notes
Chrome	93%	Not specified	High readiness contributes to overall capability.
Safari	0% (lacks support)	Not specified	Reduces global readiness to 57%.
Firefox	85%	2%	High readiness but low market share.

V. CONCLUSION

As quantum computing edges closer to reality, with Q-Day potentially arriving by 2029, the imperative for Post-Quantum Cryptography (PQC) adoption has never been more urgent. This review has traced cryptography's millennia-long evolution from ancient hieroglyphs to NIST's 2025 standards, underscoring PQC's quantum-resistant algorithms like ML-KEM, ML-DSA, and SLH-DSA as foundational defenses against vulnerabilities in legacy systems. Through diverse applications in cloud computing, finance, healthcare, government, IoT, and blockchain, PQC not only secures sensitive data but also fosters innovation in emerging technologies, ensuring resilience amid performance trade-offs.

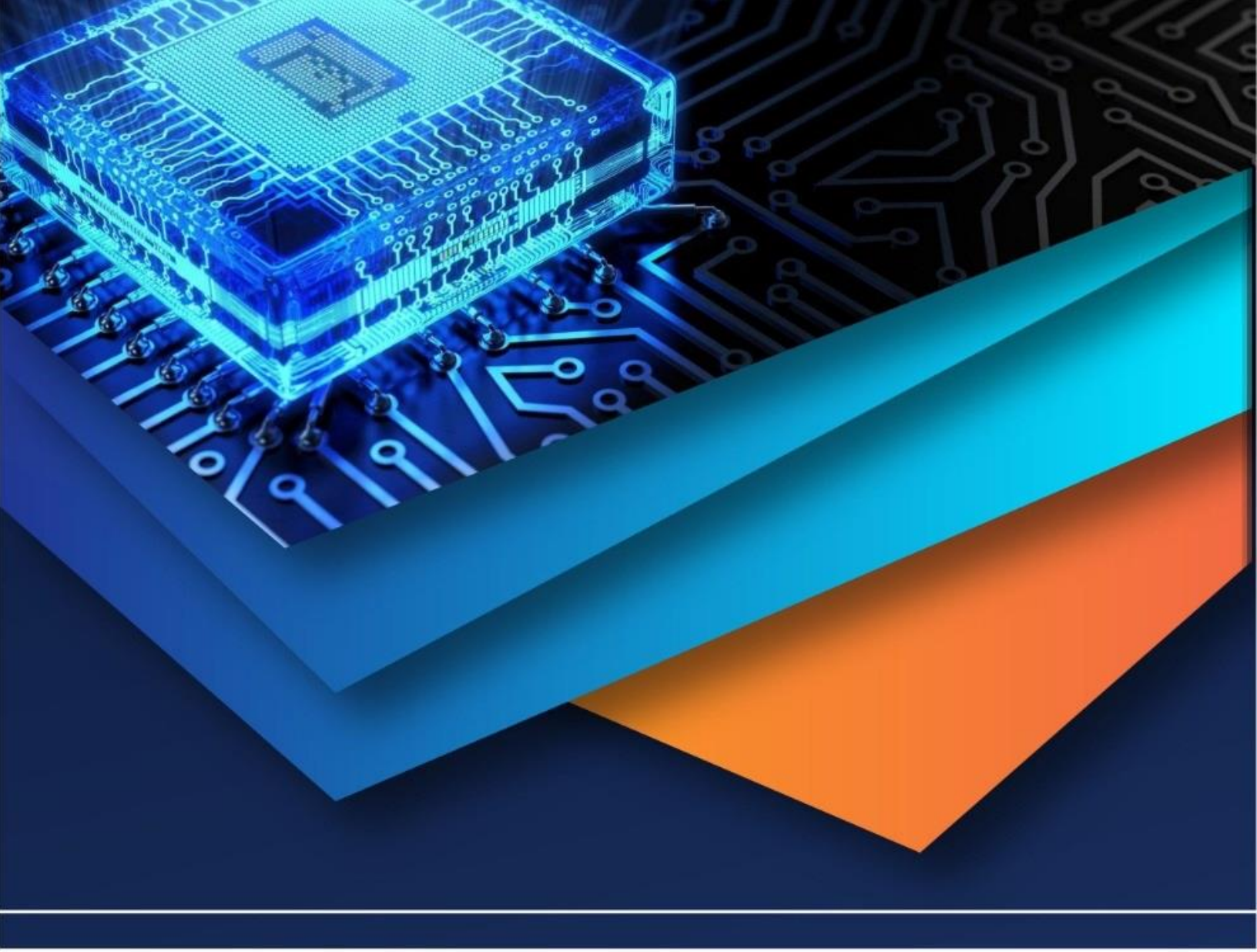
The market's explosive growth—from $0.42 billion in 2025 to projections of $29.95 billion by 2034, while Data Center market projected to top $100 B by 2027[63]—signals a transformative shift, driven by regulatory mandates and the need to mitigate trillion-dollar breach risks. In India, GCCs stand at the forefront, leveraging the National Quantum Mission to evolve into innovation powerhouses, unlocking economic value through PQC pilots and upskilling while navigating talent and cost challenges via strategic collaborations.

Ultimately, embracing PQC is not merely a technological upgrade but a strategic necessity for safeguarding the digital future. In PQC era, GCC and cloud companies will boldly rebrand themselves as quantum-resilient powerhouses, touting PQC compliance certifications—such as the emerging PQCC standard, mirroring like ISO 27001—to assure clients that their data stands to quantum threats, fostering unbreakable trust and a competitive edge. Organizations and nations that act decisively will thrive in a quantum-secure world, preserving trust, privacy and competitiveness against inevitable threats.

REFERENCES

[1] Montanaro, A. Quantum Algorithms: An Overview. npj Quantum Inf 2, 15023 (2016). https://doi.org/10.1038/npjqi.2015.23
[2] Syeda Kawsar**,** An Overview of Quantum Computing's Potential to Solve Complex Problems, December 2022, Journal of Mathematical & Computer Applications, DOI: 10.47363/JMCA/2022(1)E163**,**
[3] Manish Kumar, Post-quantum cryptography Algorithm's standardization and performance analysis, Array, Volume 15,2022,100242, https://doi.org/10.1016/j.array.2022.100242
[4] ibm, https://www.ibm.com/think/topics/cryptography-history
[5] Al-Amin Mohammed, Abdulrahman Olaniyan, Vigenere Cipher: Trends, Review and Possible Modifications, Feb 2016, International Journal of Computer Applications 135(11):46-50, DOI: 10.5120/ijca2016908549,
[6] https://www.sciencedirect.com/topics/computer-science/enigma-machine
[7] M.E. Hellman, An overview of public key cryptography, June 2002, IEEE Communications Magazine 40(5):42-49, DOI: 10.1109/MCOM.2002.1006971, IEEE Xplore,
[8] Dan Boneh, Twenty Years of Attacks on the RSA Cryptosystem, https://crypto.stanford.edu/~dabo/papers/RSA-survey.pdf
[9] Badukuri Hemalatha, Badukuri Premalatha, Buduri Reddaiah, Advanced Secure Communication: Exploring Quantum Key Distribution, the BB84 Method, April 2024, International Journal of Engineering and Advanced Technology 13(4):29-33, DOI: 10.35940/ijeat.D4434.13040424,
[10] https://postquantum.com/post-quantum/shors-algorithm-a-quantum-threat/
[11] Charles Gitonga Kinyua, European Journal of Information Technologies and Computer Science, The Impact of Quantum Computing on Cryptographic Systems: Urgency of Quantum-Resistant Algorithms and Practical Applications in Cryptography, DOI: 10.24018/ejcompute.2025.5.1.146
[12] Yong Wang, Eddie Shahril Ismail , A Review on the Advances, Applications, and Future Prospects of Post-Quantum Cryptography in Blockchain and IoT, Digital Object Identifier 10.1109/ACCESS.2025.3584473, VOLUME 13, 2025, IEEE Access
[13] https://thequantuminsider.com/2025/05/21/microsoft-brings-post-quantum-cryptography-to-windows-and-linux-in-early-access-rollout/
[14] Freyer, O., Ostermann, M., Minssen, T. et al. Quantum cryptography and data protection for medical devices before and after they meet Q-Day. npj Digit. Med. 8, 620 (2025). https://doi.org/10.1038/s41746-025-02082-3
[15] https://thequantuminsider.com/2025/05/24/google-researcher-lowers-quantum-bar-to-crack-rsa-encryption
[16] https://research.ibm.com/blog/nist-pqc-standards
[17] www.seventhsense.ai
[18] NIST, https://www.nist.gov/cybersecurity/what-post-quantum-cryptography
[19] Swati Dixit, Dr. Ujwal Ramesh Shirode, Santoshkumar Vaman Chobe, Swati Nikam, Yogita D. Bhise, The Impact of Quantum Computing on Cryptographic Security Protocols, Journal Advances in Nonlinear Variational Inequalities, Vol 27 No. 3 (2024),
[20] NIST, Module-Lattice-Based Key-Encapsulation Mechanism Standard, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.203.pdf
[21] Naya Nagy, Sarah Alnemer, Lama Mohammed Alshuhail, Haifa Alobiad, Tala Almulla, Fatima Ahmed Alrumaihi, Najd Ghadra, Marius Nagy, Module-Lattice-Based Key-Encapsulation Mechanism Performance Measurements, Sci 2025, 7(3), 91; https://doi.org/10.3390/sci7030091
[22] https://medium.com/@adnanmasood/quantum-sundays-21-federal-transition-to-post-quantum-cryptography-kyber-key-exchange-and-bb1d3137e264
[23] https://www.ipfire.org/blog/ipfire-2-29-core-update-193-released
[24] https://cloud.google.com/blog/products/identity-security/announcing-quantum-safe-key-encapsulation-mechanisms-in-cloud-kms
[25] https://aws.amazon.com/blogs/security/aws-lc-fips-3-0-first-cryptographic-library-to-include-ml-kem-in-fips-140-3-validation/
[26] https://www.encryptionconsulting.com/how-ml-dsa-replaces-ecc-and-rsa-for-digital-signatures/
[27] https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF
[28] Homer A. Riva-Cambrin, Rahul Singh, Sanju Lama Garnette R. Sutherland, Extensible Post Quantum Cryptography Based Authentication, https://arxiv.org/html/2505.16112v1
[29] https://csrc.nist.gov/pubs/fips/205/final
[30] https://www.ietf.org/archive/id/draft-tls-reddy-slhdsa-00.html
[31] https://cloud.google.com/security/resources/post-quantum-cryptography
[32] https://aws.amazon.com/security/post-quantum-cryptography/
[33] Naveen Kannegundla, Quantum-Resilient Cloud Networking: Designing Post-Quantum Secure Communication Protocols For Federated Cloud Environments In 2025, International Journal of Advanced Research in Education and Technology, Volume 12, Issue 1, January-February 2025, DOI:10.15680/IJARETY.2025.1201035,

[34] Ramesh Reddy Turpu, Fortifying Banking Transactions: Harnessing Post-Quantum Cryptography for Next-Generation Security, International Journal of Cyber Security (IJCS), 1(1), 2023, 1-9.
[35] https://www.thestack.technology/post-quantum-digital-signature-breakthrough-jp-morgan/
[36] https://eviden.com/publications/digital-security-magazine/cybersecurity-predictions-2025/post-quantum-cryptography-market-trends/
[37] SEC, Post-Quantum Financial Infrastructure Framework (PQFIF) A Roadmap for the Quantum-Safe Transition of Global Financial Infrastructure, U.S. Crypto Assets Task Force – SEC, September 03, 2025
[38] WEF, Quantum Technologies: Key Strategies and Opportunities for Financial Services Leaders WHITE PAPER JULY 2025
[39] Adebayo Yusuf Balogun, Post-Quantum Cryptography and Encryption Standards: Safeguarding Patient Data Against Emerging Cyber Threats in Telemedicine, February 2025, Asian Journal of Research in Computer Science 18(3):345-367, DOI: 10.9734/ajrcos/2025/v18i3598,
[40] Saberi Kamarposhti M, Ng KW, Chua FF, Abdullah J, Yadollahi M, Moradi M, Ahmadpour S., Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data. Heliyon. 2024 May 16;10(10):e31406. doi: 10.1016/j.heliyon.2024.e31406.
[41] https://hoop.dev/blog/hipaa-quantum-safe-cryptography-a-practical-guide-for-secure-compliance
[42] Don Roosan, Rubayat Khan, Saif Nirzhor, Fahmida Hai, Blockchain in Healthcare Today: Post-Quantum Cryptography Resilience in Telehealth Using Quantum Key Distribution, Apr 2025, DOI: 10.30953/bhty.v8.379
[43] https://thequantuminsider.com/2025/05/15/u-s-presses-federal-agencies-to-adopt-post-quantum-cryptography-in-government-acquisitions/?__cf_chl_tk=aAMFBSCPSRFkDM5dP6avjyg5A9PMIq3OCWxh98QzGLM-1761649221-1.0.1.1-LORjbXvrFQw72mMuLDr3_IunwR.2Xy07XOWfUc3hlmc
[44] GSA, 2025, Post Quantum Cryptography Buyer's Guide
[45] Kubernetes, 2025, Post-Quantum Cryptography in Kubernetes.
[46] www.finacle.com/recent reports
[47] NIST, https://www.nist.gov/news-events/news/2025/08/nist-finalizes-lightweight-cryptography-standard-protect-small-devices
[48] A. Sharma, S. Rani, Post-Quantum Cryptography (PQC) for IoT-Consumer Electronics Devices Integrated With Deep Learning, in IEEE Transactions on Consumer Electronics, vol. 71, no. 2, pp. 4925-4933, May 2025, doi: 10.1109/TCE.2025.3569904
[49] https://medium.com/be-tech-with-santander/how-to-configure-post-quantum-cryptography-in-your-web-server-fcf79e05e526
[50] Chen, Y., et al., Quantum Computing Empowering Blockchain, Journal of Cloud Computing, 2025, 14(25).
[51] https://thequantuminsider.com/2025/01/04/solana-takes-a-step-toward-pqc-era-with-quantum-resistant-vault/
[52] Batta, P., Wasson, V., Sardar, S., Securing Blockchain with Quantum-Inspired Protocols. In: Kumar, A., Batta, P., Le, DN. (eds) Quantum Protocols in Blockchain Security. Blockchain Technologies. Springer 2025, Singapore. https://doi.org/10.1007/978-981-96-9148-7_1
[53] Nadeem Ahmed, Lei Zhang, Aryya Gangopadhyay, A Survey of Post-Quantum Cryptography Support in Cryptographic Libraries, , https://arxiv.org/html/2508.16078v1
[54] https://www.imarcgroup.com › post-quantum-cryptography
[55] https://www.marketsandmarkets.com/Market-Reports/post-quantum-cryptography-market-126986626.html
[56] https://inductusgcc.com › how-the-best-gccs-in-india-ar
[57] www.ibef.com
[58] https://etedge-insights.com › GCC
[59] https://inductusgcc.com/quantum-ready-gccs-preparing-for-tomorrows-computing-powerhouses/
[60] Medium, Top 10 Post-Quantum Cryptography Vendors, 2025
[61] F5 Labs, 2025, The State of Post-Quantum Cryptography on the Web, https://www.f5.com/labs/articles/the-state-of-pqc-on-the-web
[62] https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.204.pdf
[63] Times of India, 3rd Nov, 2025, Pune Edition



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY