Barrett-danes and Ahmad *Discover Applied Sciences* (2025) 7:1083
https://doi.org/10.1007/s42452-025-07322-5

Discover Applied Sciences

REVIEW **Open Access**

Quantum computing and cybersecurity: a rigorous systematic review of emerging threats, post-quantum solutions, and research directions (2019–2024)

Freddie Barrett-danes[1] and Fahad Ahmad[1,2*]

*Correspondence:
Fahad Ahmad
fahad.ahmad@port.ac.uk
[1]School of Computing, Faculty of Technology, University of Portsmouth, Winston Churchill Ave, Southsea, Portsmouth PO1 3HE, UK
[2]Portsmouth Artificial Intelligence and Data Science Centre (PAIDS), University of Portsmouth, Portsmouth PO1 3HE, UK

Abstract
This systematic review examines the transformative impact of quantum computing (QC) on cybersecurity by analysing peer-reviewed literature published between 2019 and 2024. The study identifies the most pressing emerging threats, particularly the vulnerability of classical cryptographic systems to quantum algorithms such as Shor's and Grover's. It assesses the current state of post-quantum cryptography (PQC) solutions, including lattice-based schemes and hybrid frameworks integrating quantum key distribution (QKD). The originality of this work lies in its focus on synthesizing research across disciplines while critically evaluating implementation readiness, economic feasibility, and scalability particularly for internet of things (IoT) environments. Key contributions include the integration of real-world pilot case studies, a preferred reporting items for systematic reviews and meta-analyses (PRISMA) -based methodological framework, and a strategic outlook for interdisciplinary collaboration. This review provides significant insight into the evolving cybersecurity landscape and offers robust recommendations for policymakers, researchers, and practitioners aiming to navigate the quantum era with confidence.

Keywords Quantum computing, Cybersecurity, Post-quantum cryptography (PQC), Quantum key distribution (QKD), Cryptographic systems, Emerging threats, Quantum vulnerability, Hybrid cryptographic models, Internet of things (IoT), Interdisciplinary collaboration, Preferred reporting items for systematic reviews and meta-analyses (PRISMA), Implementation feasibility

1 Introduction

Quantum computing (QC) represents a paradigm shift in computational capabilities, offering transformative potential across domains such as drug discovery, materials science, logistics, and finance. For instance, QC's capacity to simulate molecular structures and quantum interactions allows for unprecedented advancements in drug development and protein folding research [1]. However, alongside these breakthroughs lies an equally powerful threat to digital security infrastructure [2]. As QC continues to advance, it exposes fundamental vulnerabilities in the cryptographic algorithms that underpin global cybersecurity.

Classical cryptographic systems are rooted in computational hardness assumptions Rivest–Shamir–Adleman (RSA) encryption relies on the difficulty of factoring large integers, and Advanced Encryption Standard (AES) is secured through symmetric key operations resistant to classical brute-force attacks. However, quantum algorithms have undermined these foundations: Shor's algorithm compromises RSA by enabling efficient integer factorization, while Grover's algorithm reduces AES's effective key length, enhancing brute-force efficiency [3, 4]. The impact is not theoretical alone; the trajectory of quantum hardware development points toward practical decryption capabilities within the next decade [5].

In response, the National Institute of Standards and Technology (NIST) launched a multi-year effort to standardize post-quantum cryptography (PQC) algorithms that remain secure against both classical and quantum threats. Despite the finalization of four PQC algorithms in 2024, the process revealed critical insights: two previous candidates were compromised during testing, with one broken in under an hour [6], and even the approved algorithms require further real-world validation and optimization for constrained environments [7].

This review presents an original, structured synthesis of the literature on quantum-era cybersecurity threats, PQC development, and implementation challenges. Guided by the preferred reporting items for systematic reviews and meta-analyses (PRISMA) framework, the review applies rigorous inclusion criteria and quality assessment methods to evaluate academic and emerging industry contributions. Key themes addressed include algorithmic readiness, interoperability issues, economic feasibility, and deployment barriers in sectors such as the internet of things (IoT), finance, and healthcare. The review also contributes a novel conceptual model mapping quantum threats to PQC and quantum key distribution (QKD) mitigation strategies and identifies opportunities for interdisciplinary research collaborations.

1.1 Background

Cybersecurity in the digital era comprises multi-layered systems addressing network integrity, data protection, and access control. At its core lies cryptography mathematical techniques that ensure confidentiality, authenticity, and integrity of data transmission. RSA, grounded in prime factorization, and AES, based on substitution-permutation structures, have long served as foundational encryption methods [8, 9]. Classical computers lack the power to brute-force such schemes efficiently, preserving the trust in global communication networks [10].

QC, illustrated in Fig. 1, leverages quantum mechanical principles i.e., entanglement and superposition [11, 12] to perform operations at a scale exponentially faster than classical counterparts. This capability enables algorithms like Shor's and Grover's to bypass the computational barriers upon which current encryption relies [3, 13]. The result is a paradigm in which legacy cryptographic systems are no longer secure by design.

While the immediate threat of quantum decryption is tempered by the technical limitations of today's QC hardware [15], experts project that within a decade, machines capable of breaking classical encryption may emerge [5]. Recognizing this, NIST

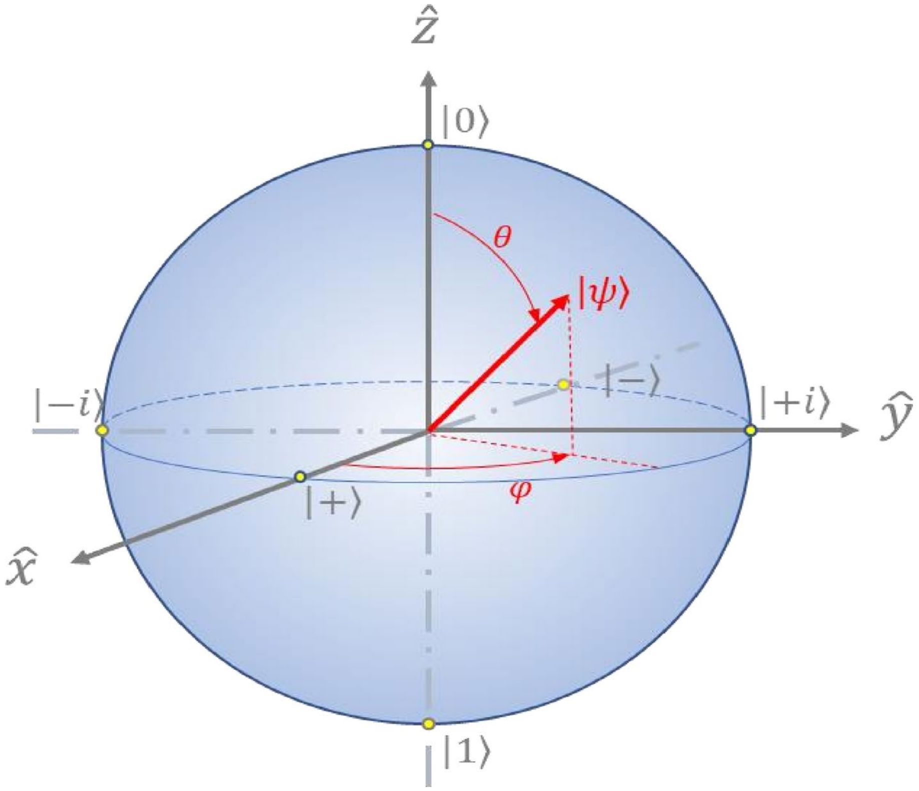


Fig. 1 Qubit visualization [14]

initiated a global collaboration to develop PQC standards [16], leading to the publication of lattice-based, hash-based, and code-based algorithms [17]. However, practical deployment remains challenged by resource demands, lack of industry readiness, and the need for widespread infrastructure upgrades [18].

A particularly urgent concern is the adoption of the "store-now-decrypt-later" (SNDL) model, where adversaries intercept encrypted communications today with the intent of decrypting them using future quantum capabilities [19]. This underscores the pressing need for proactive migration to quantum-safe protocols and calls for a unified effort by academia, government, and industry to secure the global digital ecosystem before practical quantum threats fully materialize.

1.2 Aims and objectives

This systematic review aims to comprehensively assess the implications of QC for cybersecurity. By applying a structured approach grounded in the Population, Interest, Context (PICo) methodology (see Table 1), this review seeks to:

1. Identify and categorize emerging quantum computing threats:
   Analyse recurring threat patterns, categorizing them based on implications for cryptographic frameworks, sector-specific vulnerabilities, and broader impacts on cyberspace.
2. Evaluate the readiness and practicality of post-quantum cryptographic (PQC) solutions:

Table 1 PICo (population, interest, context) framework

P (Population)	I (Interest)	Co (Context)
Cybersecurity systems and frameworks	Impact and threats of quantum computing advancements	Peer-reviewed technical literature and research (2019–2024)
Encryption systems and protocols	Capabilities of quantum algorithms (e.g., Shor's, Grover's)	Journals, conferences, and scholarly articles
Security infrastructure	Quantum-based security breaches and attack methodologies	English-language sources only
Network security and data protection	Post-quantum cryptographic (PQC) implementations	Focused on emerging threats, mitigations, and implementation readiness
Authentication and access control systems	Development of quantum key distribution (QKD) and hybrid cryptographic models	Emphasis on practical scenarios, including economic and scalability considerations
Digital communication and IoT systems	Interdisciplinary strategies and transition planning	Documents detailing implementation scenarios and deployment challenges in real-world environments

Description: Examine the effectiveness, scalability, and deployment readiness of various PQC algorithms, quantum key distribution (QKD) models, and hybrid cryptographic architectures.

3. Highlight existing research gaps and implementation barriers:
   Identify limitations in current research and practice, including lack of interdisciplinary collaboration, scalability challenges in constrained environments, and the absence of large-scale real-world testing.

1.3 Research questions

To achieve these objectives, this review addresses the following key research questions:

1. What are the most immediate quantum threats to current cryptographic systems and sector-specific cybersecurity?
2. How effective and scalable are the proposed PQC and QKD solutions in securing current systems?
3. What research gaps and implementation challenges exist in transitioning to quantum-resilient cybersecurity frameworks?

1.4 Contribution of the study

This review contributes a comprehensive and structured synthesis of the current literature on quantum computing's impact on cybersecurity between 2019 and 2024. It distinguishes itself through its rigorous application of the PICo framework and PRISMA methodology, ensuring both transparency and methodological depth. By identifying, categorizing, and evaluating emerging quantum threats and PQC solutions, the study offers original insights into the readiness of various mitigation approaches and uncovers underexplored research gaps. Moreover, the inclusion of real-world case studies, discussion on economic feasibility, and interdisciplinary recommendations enhances the practical significance of the findings for researchers, policymakers, and cybersecurity professionals preparing for the quantum era.

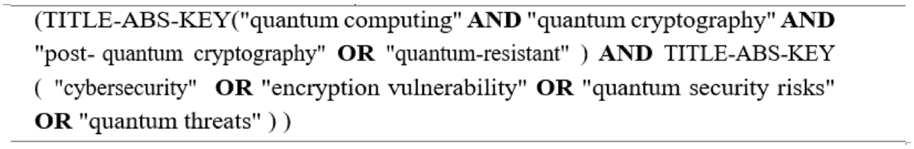
1.5 Structure of the review

The remainder of this review is organized into the following sections. Section 2 outlines the methodology used to conduct this systematic review, including the application of

Table 2 List and categories of keywords

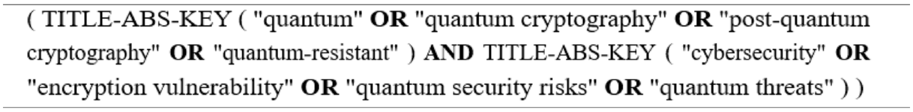
Quantum computing focus	Cybersecurity focus
Quantum computing	Cybersecurity
Quantum cryptography	Encryption vulnerability
Post-quantum cryptography	Quantum security risks
Quantum-resistant	Quantum threats

Table 3 Final search



(TITLE-ABS-KEY("quantum computing" **AND** "quantum cryptography" **AND** "post- quantum cryptography" **OR** "quantum-resistant") **AND** TITLE-ABS-KEY ("cybersecurity" **OR** "encryption vulnerability" **OR** "quantum security risks" **OR** "quantum threats"))

Table 4 Penultimate search



(TITLE-ABS-KEY ("quantum" **OR** "quantum cryptography" **OR** "post-quantum cryptography" **OR** "quantum-resistant") **AND** TITLE-ABS-KEY ("cybersecurity" **OR** "encryption vulnerability" **OR** "quantum security risks" **OR** "quantum threats"))

the PICo framework, study selection criteria, and quality assessment strategy. Section 3 presents the results, highlighting thematic clusters in the literature and providing key statistics and trends across the included studies. Section 4 delivers an in-depth discussion of the findings, addressing major challenges such as scalability, real-world implementation, and interdisciplinary collaboration, while also outlining the limitations of this review. Finally, Sect. 5 concludes the review by summarizing the core insights and proposing forward-looking recommendations for future research and implementation.

2 Methodology

2.1 Search strategy

The first step in this review was identifying a database to search for this; SCOPUS was chosen. This was ideal due to the comprehensive coverage of scientific literature across multiple disciplines, which is essential when researching a field such as QC, which encompasses many different areas of science and technology [20]. It also allows for easy use with external tools such as Rayyan, which was also used to conduct screening and export the search for further analysis.

After identifying the database, the keywords were then selected. The keywords were broken into two focuses to encompass the intersection of QC and cybersecurity (see Table 2). The final search (see Table 3) utilized the AND/OR functions to balance the scope of the review. This is demonstrated by the penultimate search (see Table 4) utilizing the OR operator to a greater extent, which returned 698 results. In contrast, the final result had 84 results by leveraging the AND operator to a greater extent. This strategy enabled the refined collection of papers to apply the exclusion and inclusion criteria.

2.2 Inclusion/exclusion criteria

To ensure the relevance and quality of the final selection of papers, a multi-tiered inclusion and exclusion process was adopted:

Inclusion Criteria:

1. Relevance to Quantum Computing and Cybersecurity:
   Studies must address both fields explicitly and contain relevant keywords in the title, abstract, or keyword section.
2. Publication Year:
   Only papers published between 2019 and 2024 were included to focus on the most recent and peer-reviewed developments.
3. Source Type:
   Only peer-reviewed journal articles and conference papers were selected to ensure scientific credibility and original contributions.
4. Subject Area:
   Papers categorized under Computer Science were prioritized to maintain a technical and cybersecurity-focused perspective.
5. Language:
   Only English-language publications were considered to ensure consistency and accessibility.

Exclusion Criteria (Applied Post-Search):

1. Irrelevant Topics:
   Papers that did not address the intersection of QC and cybersecurity, or focused exclusively on niche, domain-specific applications, were excluded.
2. Unavailable Full Text:
   Studies for which the full text could not be accessed or reviewed due to institutional restrictions were omitted.

After applying these criteria, the initial dataset of 84 papers was filtered down to 53 high-quality and relevant sources for full-text screening and thematic analysis. This ensured methodological rigor and consistency in alignment with the PRISMA framework.

2.3 Data extraction

The data extraction phase formed a critical component of this systematic review, ensuring that insights collected from each included study aligned precisely with the review's objectives and supported transparent synthesis. A structured data extraction template was designed and implemented using a standardized spreadsheet, aligning with best practices outlined in the PRISMA guidelines. This template included fields for bibliographic information (e.g., authors, year, publication type), study focus, methodology, use case context, core contributions, and stated limitations.

Each paper was read in full, and data were independently extracted by reviewers using Rayyan, a widely adopted collaborative tool for systematic reviews. This platform allowed real-time tagging, blind screening, and conflict resolution, significantly enhancing the consistency and reproducibility of the process [21]. Additionally, notes and highlights were annotated for all papers to ensure traceability and transparency of qualitative interpretation.

To facilitate targeted analysis, each study was categorized under one or more of three thematic groups that directly correspond to the review's core research questions: Emerging Quantum Threats, Post-Quantum Solutions, and Research Gaps. Within these themes, extracted data included specific quantum algorithms (e.g., Shor's, Grover's), types of cryptographic protocols impacted (e.g., RSA, AES, lattice-based PQC), sectors involved (e.g., IoT, healthcare, finance), and evaluation metrics such as scalability, performance, or implementation challenges.

Quantitative data points such as algorithm benchmarks, deployment timelines, or test environments were captured to support comparative analysis in Sect. 3. Qualitative themes, including author recommendations, conceptual models, or implementation barriers, were codified using an inductive coding approach to generate a robust thematic framework.

This methodical extraction not only ensured high fidelity in reporting findings but also laid the foundation for structured synthesis and interpretation in the following sections. It also supports reproducibility, which is essential given the evolving nature of the quantum cybersecurity landscape.

2.4 Quality assessment

The studies' quality was assessed primarily by focusing on peer-reviewed research to ensure scientific rigor and reliability [22]. Peer-reviewed journal articles and conference papers were part of the inclusion/exclusion criteria to guarantee this. This meant that all papers from the search met this standard before screening even began. However, it is worth noting that peer review alone has limitations; bias can be present even in the peer review process, and a poor review process impacts this assumed quality [23].

During the screening, studies were evaluated on their relevance to the objectives of this review and their value to the discussion that could be gained. Domain-specific or irrelevant studies that did not address the intersection of cybersecurity and QC were excluded. Also, papers that the reviewer could not access were not included, as there was no way to guarantee the relevance or value of this review.

Scopus reinforced the high standard of research assumed, as it is known for its comprehensive collection of peer-reviewed studies. This ensured that the studies included in this review were of sufficient quality to form a reliable foundation for analysis.

3 Results

3.1 Study selection

To ensure methodological rigor and enhance transparency, this review followed the PRISMA framework as a foundational structure. The study selection process was conducted in four key stages: identification, screening, eligibility assessment, and final inclusion, each of which is clearly outlined in the PRISMA-compliant flow diagram (see Fig. 2).

An initial search of the SCOPUS database using carefully constructed Boolean queries identified 84 records. These results were then subjected to a structured screening process based on predefined inclusion and exclusion criteria (Sect. 2.2), ensuring alignment with the review's focus on QC and cybersecurity. Following full-text review and quality appraisal, a final set of 53 peer-reviewed articles was included for in-depth thematic analysis.

The PRISMA-based process enhanced consistency and reproducibility, supporting a transparent audit trail for selection decisions and reinforcing the systematic nature of this review.

After applying the predefined inclusion and exclusion criteria outlined in Sect. 2.2, a total of 31 documents were excluded during the screening stage due to lack of relevance

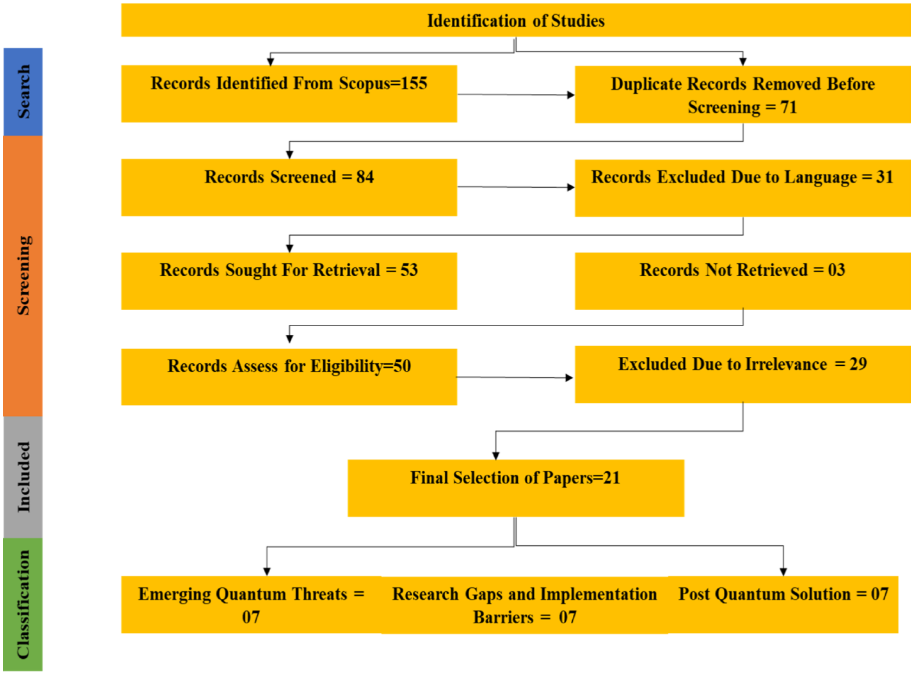
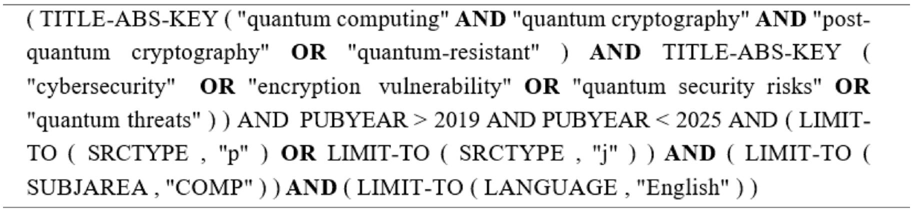

Search
Screening
Included
Classification
Identification of Studies
Records Identified From Scopus=155
Duplicate Records Removed Before Screening = 71
Records Screened = 84
Records Excluded Due to Language = 31
Records Sought For Retrieval = 53
Records Not Retrieved = 03
Records Assess for Eligibility=50
Excluded Due to Irrelevance = 29
Final Selection of Papers=21
Emerging Quantum Threats = 07
Research Gaps and Implementation Barriers = 07
Post Quantum Solution = 07

Fig. 2 PRISMA Literature Search and Selection Method Diagram

Table 5 Final search with inclusion/exclusion criteria



(TITLE-ABS-KEY ("quantum computing" **AND** "quantum cryptography" **AND** "post-quantum cryptography" **OR** "quantum-resistant") **AND** TITLE-ABS-KEY ("cybersecurity" **OR** "encryption vulnerability" **OR** "quantum security risks" **OR** "quantum threats")) AND PUBYEAR > 2019 AND PUBYEAR < 2025 AND (LIMIT-TO (SRCTYPE , "p") **OR** LIMIT-TO (SRCTYPE , "j")) **AND** (LIMIT-TO (SUBJAREA , "COMP")) **AND** (LIMIT-TO (LANGUAGE , "English"))

or methodological fit (see Table 5). This ensured that only studies meeting the core criteria pertaining directly to QC and cybersecurity were retained for full-text analysis.

The remaining 53 papers underwent a second round of screening. Reports that could not be retrieved were excluded at this stage due to lack of access; specifically, three papers were removed on this basis. The remaining studies were then assessed for thematic relevance and contribution to the overarching research objectives of this review. Domain-specific publications that did not explicitly address the intersection of QC and cybersecurity were also excluded. This rigorous screening process resulted in a final dataset of 21 high-quality studies (see Table 6). To facilitate structured analysis, the selected papers were subsequently classified into three thematic subcategories, and overlapping concepts and recurring trends were systematically identified for synthesis in the Results and Discussion sections.

Here is a thematic breakdown of the 21 included studies:

1. *Post-Quantum Solutions* dominate the research landscape, reflecting a strong focus on the development, evaluation, and deployment of lattice-based, hybrid, and blockchain-integrated cryptographic frameworks.

Table 6 Included reports

Title	Authors	Year	Document type
An Electoral Exception? Quantum Computing Readiness and Internet Voting	Rodríguez-Pérez et al. [24]	2024	Journal Article
Securing the Future: A Comprehensive Review of Post-Quantum Cryptography and Emerging Algorithms	Allgyer et al. [17]	2024	Conference
The Quantum Threat: Implications for Data Security and the Rise of Post-Quantum Cryptography	Tiwari et al. [25]	2024	Conference
Enhancing Cloud Security Based on the Kyber Key Encapsulation Mechanism	Altarawni et al. [26]	2024	Journal Article
A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats	Yalamuri et al. [27]	2022	Conference
Lattice-Based Cryptography and NTRU: Quantum-Resistant Encryption Algorithms	Nisha et al. [28]	2024	Conference
Applied Post-Quantum Secure Method for IoT Devices: A Case Study for Autonomous Vehicles Communication	Figlarz et al. [29]	2022	Conference
Post-Quantum Cryptography Algorithm's Standardization and Performance Analysis	Kumar [30]	2022	Journal Article
Modular Blockchain Architecture: Securing Data with Quantum-Safe Encryption	Pabla and Sultana [31]	2024	Conference
Navigating Quantum Security Risks in Networked Environments: A Comprehensive Study of Quantum-Safe Network Protocols	Baseri et al. [32]	2024	Journal Article
Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective	Oliva del Moral et al. [33]	2024	Journal Article
Secure Keys Data Distribution-Based User-Storage-Transit Server Authentication Using PQC Methodology	Henge et al. [34]	2023	Journal Article
Cryptographic Algorithms for IoT Devices: A Quantum Analysis	Alam et al. [35]	2024	Conference
A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies	Hasan et al. [36]	2024	Conference
FIPS Compliant Quantum Secure Communication Using Quantum Permutation Pad	He et al. [37]	2023	Journal Article
PQC Secure: Strategies for Defending Against Quantum Threats	Jenefa et al. [38]	2023	Conference
Exploring the Fusion of Lattice-Based QKD for Secure IoT Communications	Biswas et al. [39]	2024	Journal Article
Transforming Military Security: Quantum Age Blockchain Architecture for IoBT-PARS	Çakal and Özdemir [40]	2024	Conference
Improving OTP Authentication with PQC Algorithms	Khorkheli et al. [41]	2024	Conference
Integrating PQC and Blockchain to Secure Low-Cost IoT Devices	Castiglione et al. [42]	2024	Journal Article
Distributed Cyber-Infrastructures and AI in the Hybrid Post-Quantum Era	Yavuz et al. [43]	2022	Conference

2. *Emerging Quantum Threats* are explored in a smaller subset, addressing the vulnerabilities introduced by quantum algorithms like Shor's and Grover's.
3. Only a single study directly addresses *Research Gaps and Implementation Barriers*, underscoring a notable shortfall in practical assessments, scalability analyses, and interdisciplinary readiness.

3.2 Descriptive statistics

The 21 studies included in the screening process were analysed to understand the descriptive statistics of the papers. The first statistic was the type of report that was more present in the included studies (see Fig. 3). Most of these were conference papers, making up 57.14% of the sample, with the other 42.86% being journal articles.

Interestingly, although the search included papers from 2019 to 2024, the final set of documents only had papers as late as 2022 (see Fig. 4). This indicates that research in

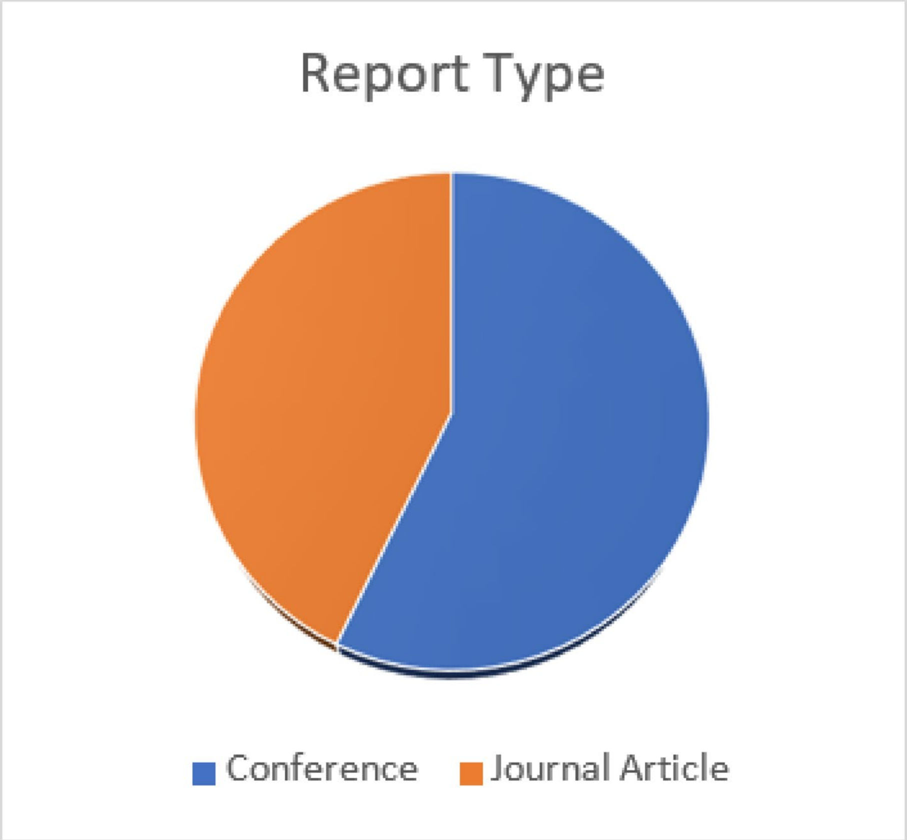


Fig. 3 Distribution of included studies by document type (N = 21)

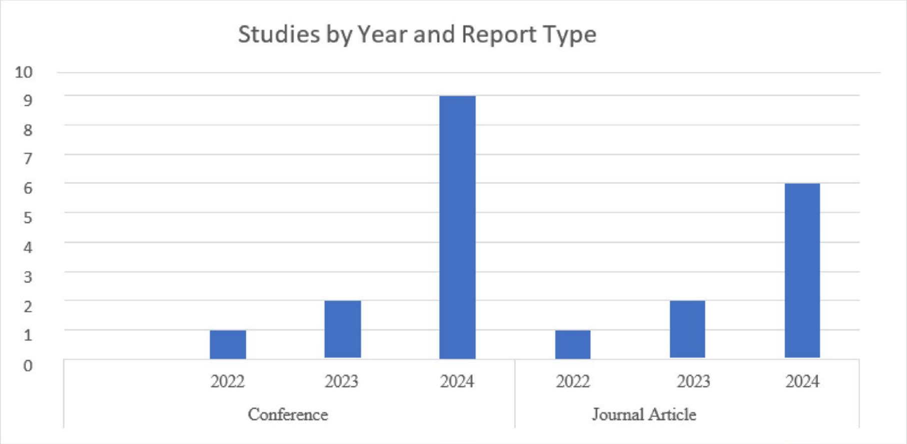


Fig. 4 Distribution of selected studies by year grouped by document type (N = 21)

this field has significantly increased in recent years, likely due to the growing recognition of QC's implications on cybersecurity. Most papers are from 2024 (15 out of 21), highlighting that this is an increasingly researched topic as it becomes a more publicly reported phenomenon, attracting more attention from researchers and industries to investigate the risks posed by QC.

As outlined in the previous section, the final set of 21 studies was systematically categorized into three thematic clusters for analytical clarity: emerging quantum threats, post-quantum solutions, and research gaps and implementation barriers. This thematic classification reflects the evolving research priorities in quantum-era cybersecurity and facilitates a more nuanced synthesis of the field's current direction (see Fig. 5).

A clear majority of the studies 17 out of 21 (81.0%) fell under the PQC solutions category, indicating a dominant focus on the development, evaluation, and optimization of cryptographic frameworks resistant to quantum attacks. These solutions include lattice-based encryption schemes, QKD integrations, and hybrid models leveraging blockchain or lightweight cryptography. This prevalence suggests that the academic and industrial communities are investing significant effort into proactively mitigating the vulnerabilities introduced by quantum algorithms such as Shor's and Grover's.

In contrast, only three studies (14.3%) were classified under emerging quantum threats, focusing primarily on characterizing the nature, scope, and urgency of the security risks posed by advances in QC. These studies serve a critical foundational role, as they contextualize the urgency for PQ solutions by outlining how quantum technologies compromise existing cryptographic standards like RSA, ECC, and AES.

The most underrepresented theme was research gaps and implementation barriers, with only one study (4.8%) directly addressing the practical challenges of transitioning to quantum-resilient infrastructures. This finding highlights a pressing shortfall in the literature: while the theoretical robustness of PQC solutions is being extensively explored, significantly fewer studies assess their real-world feasibility, economic cost, scalability for resource-constrained environments (e.g., IoT), and interdisciplinary implementation strategies.

This thematic imbalance underscores a critical need for further research dedicated to bridging the gap between theory and practice. Without substantial empirical testing, cost–benefit analysis, and cross-sector collaboration, even the most mathematically secure algorithms may fall short in practical deployment. Addressing these research gaps will be essential to ensuring that quantum-resilient solutions are not only theoretically sound but also adaptable, scalable, and economically viable in the global cybersecurity landscape.

The final descriptive attribute examined was the geographical distribution of the included studies, offering insights into the global research landscape surrounding QC and cybersecurity (see Fig. 6). The analysis revealed that India emerged as the leading contributor, with a notable concentration of conference papers and technical

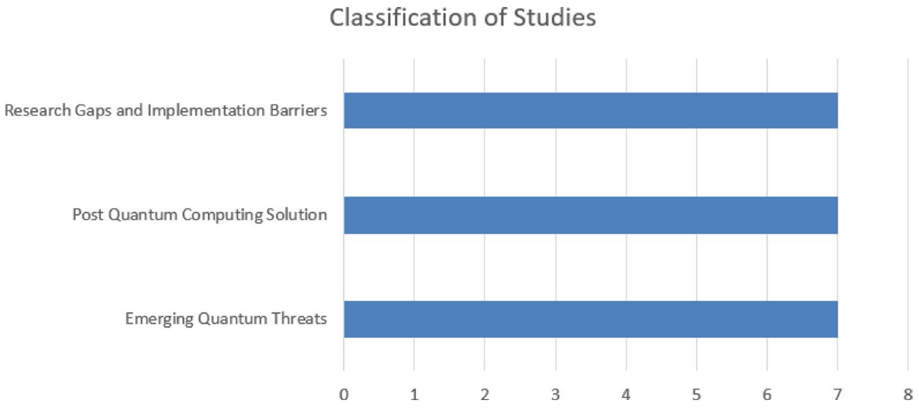


Fig. 5 Thematic classification of included studies (n = 21): emerging quantum threats, post-quantum solutions, and research gaps & barriers

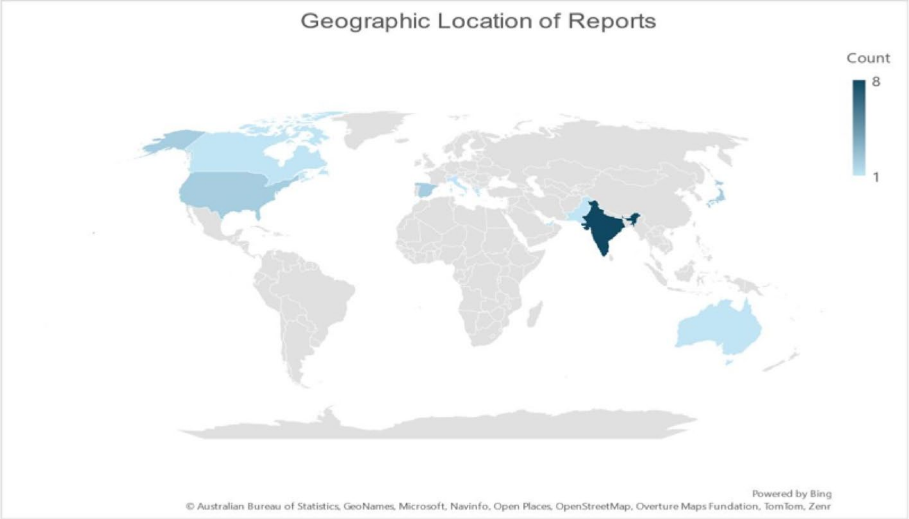

Geographic Location of Reports
Count
8
1
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenr

Fig. 6 Geographical distribution of included studies based on country of lead authorship or institutional affiliation (N = 21)

contributions originating from Indian institutions and academic consortia. This regional concentration suggests a strong institutional and academic investment in quantum-resilient cybersecurity research within the country.

In contrast, contributions from other regions were markedly lower, with most countries represented by only one or two studies each. These included select contributions from the United States, the United Kingdom, China, Germany, and a few other European and Asia–Pacific countries. While this distribution affirms that the topic is of global significance, the relatively narrow geographical footprint of peer-reviewed contributions suggests that scholarly engagement with quantum-era cybersecurity remains uneven across regions.

This geographic skew raises two important implications. First, it highlights the urgent need for broader international collaboration in order to capture a more diverse range of technological, policy, and implementation contexts. Effective mitigation of quantum threats will ultimately depend on the interoperability and adaptability of cryptographic standards across national and sectoral boundaries something that cannot be achieved without widespread global participation.

Second, the dominance of one regional research hub may inadvertently result in overrepresentation of local technological priorities, limiting the field's ability to generalize findings across diverse infrastructures, economies, and legal frameworks. A globally coordinated research effort drawing upon both developed and developing nations is therefore essential not only for identifying robust technical solutions but also for addressing the socio-economic, regulatory, and infrastructural dimensions of implementing post-quantum cybersecurity at scale.

3.3 Findings

3.3.1 Emerging quantum threats

The reviewed literature underscores the increasingly tangible risks that QC poses to classical cryptographic systems. At the core of these threats are quantum algorithms Shor's algorithm, which enables efficient factorization of large prime numbers, thereby rendering RSA and elliptic curve cryptography (ECC) obsolete; and Grover's algorithm, which accelerates brute-force attacks on symmetric encryption schemes such as AES, effectively halving their key security strength.

A consistent theme across studies is the sector-specific vulnerability of critical systems. For instance, [24] explored the exposure of internet voting infrastructures in countries such as Canada, Estonia, France, and Switzerland. Their analysis revealed long-term privacy risks and the potential for electoral compromise, particularly under scenarios where encrypted ballots may be stored and later decrypted once adversaries acquire quantum capabilities. The authors also highlighted a key gap in the field: a lack of consensus on hybrid mitigation strategies, such as combining traditional and post-quantum encryption, due to diverging views on interoperability, trust models, and implementation pathways.

Industrial sectors are equally exposed. The research [33] examined critical infrastructure systems, especially those that integrate legacy technologies commonly seen in sectors like energy, water treatment, and manufacturing. These systems are often deeply embedded, costly to replace, and lack built-in support for modern encryption protocols. As a result, their increasing connectivity to external networks often for automation or remote control has inadvertently created expanded attack surfaces, now vulnerable to both classical and quantum-enabled cyber intrusions.

The broader implications of QC on data confidentiality and system resilience are further analysed by [25], who specifically identified RSA as a cryptographic scheme on the brink of obsolescence. The study advocates for pre-emptive investment in PQC solutions, urging stakeholders not to wait for quantum hardware to reach full maturity before acting. The authors emphasize that a reactive approach could leave critical data and communications exposed during the transition period.

Another high-priority threat theme emerging across several studies is the SNDL tactic. This strategy involves malicious actors intercepting and archiving encrypted communications today with the explicit intent of decrypting them in the future using quantum computers. The study [37] stressed the severity of this threat, particularly in domains handling long-lifecycle data such as financial transactions, medical records, or intellectual property. The delayed compromise of this data could result in massive breaches of privacy, financial loss, and national security exposure [44].

Collectively, these studies paint a compelling picture of the quantum threat landscape not as a distant theoretical risk, but as a rapidly approaching reality. The convergence of high-value, long-retention data and increasingly capable quantum prototypes makes proactive defence not just desirable, but imperative. Without swift and coordinated responses, the confidentiality, authenticity, and integrity of digital systems worldwide may face unprecedented disruption.

3.3.2 Post-quantum solutions

PQC solutions represent the most extensively covered theme across the reviewed literature, reflecting the field's urgent focus on identifying and implementing cryptographic protocols resistant to quantum attacks. Most studies explore a combination of lattice-based encryption, QKD, and hybrid cryptographic frameworks, signalling a shift from theoretical exploration to practical experimentation.

A key development highlighted in multiple papers is the NIST-led standardization process, which culminated in the selection of several PQC finalist algorithms in 2024. The study [7] emphasized the global significance of these outcomes, particularly in fostering interoperability and guiding industry compliance. Complementing this, [30] provided detailed performance benchmarking of lattice-based schemes, noting their strength in security and computational efficiency. However, significant limitations remain, particularly in resource-constrained environments such as IoT and embedded systems.

Applied case studies also feature prominently. Th research [29] tested NTRUEncrypt and NTRUSign in autonomous vehicle networks, reporting enhanced encryption resilience but also citing issues with increased message length and reduced communication throughput. Similarly, [39] proposed a hybrid lattice-QKD solution for healthcare IoT, demonstrating strong performance under constrained conditions but raising flags over scalability and interoperability across legacy systems.

Innovative frameworks leveraging blockchain and PQC are gaining traction. Th study [31] introduced a PQC-QKD blockchain model for secure IoT transactions, improving latency and scalability while requiring substantial hardware investment. In the cloud domain [45, 46], evaluated the Kyber key encapsulation mechanism (KEM), highlighting its compact key size and low computational load, but noted that broader standardization and policy alignment are still needed for widespread adoption.

These findings collectively illustrate that while technical advancements in PQC are accelerating, real-world readiness is still hindered by integration, cost, and ecosystem maturity.

3.3.3 Research gaps

Despite meaningful advancements in post-quantum cryptography (PQC), several critical gaps continue to hinder its widespread adoption, particularly at scale. Among the most pressing challenges is scalability. While studies such as [42] demonstrate that PQC algorithms perform effectively in controlled or small-scale IoT environments, scaling these systems to real-world, multi-layered infrastructures remains difficult. Similarly, [33] noted that most current deployments are limited to lab-based or simulated environments, undermining the practical relevance and generalizability of these findings.

A second notable gap lies in the lack of interdisciplinary integration. Another study [43] advocated for combining PQC with artificial intelligence (AI) and machine learning (ML), yet actual implementations remain sparse. Contemporary AI-driven security frameworks such as ML-based botnet detection [47], blockchain-enhanced threat intelligence [48], and explainable Android malware detectors [49] are typically developed in isolation from quantum-resilient architectures. This disjointed approach results in fragmented security solutions and underscores the need for integrated, cross-domain cryptographic strategies tailored to the quantum era.

Sector-specific infrastructures, particularly financial systems, are similarly underexplored. Although promising proposals such as QKD-enabled ATM networks [50] exist, broader frameworks for implementing PQC across banking, e-commerce, and payment systems remain underdeveloped. Another research [36] proposed a conceptual migration framework to guide PQC adoption, but their study fell short of addressing the technical and operational complexities associated with transitioning legacy systems.

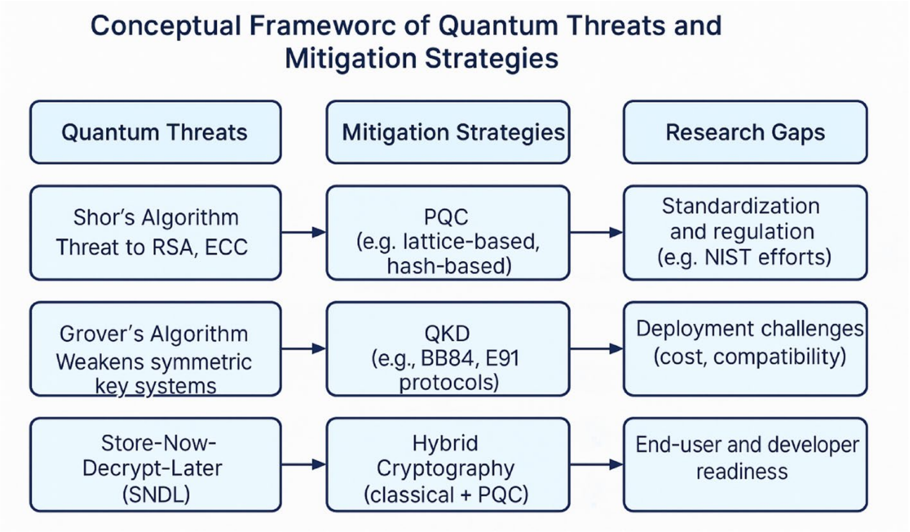

Conceptual Frameworc of Quantum Threats and Mitigation Strategies
Quantum Threats
Mitigation Strategies
Research Gaps
Shor's Algorithm Threat to RSA, ECC
PQC (e.g. lattice-based, hash-based)
Standardization and regulation (e.g. NIST efforts)
Grover's Algorithm Weakens symmetric key systems
QKD (e.g., BB84, E91 protocols)
Deployment challenges (cost, compatibility)
Store-Now-Decrypt-Later (SNDL)
Hybrid Cryptography (classical + PQC)
End-user and developer readiness

Fig. 7 Conceptual framework of quantum threats and mitigation strategies

A third and increasingly urgent area of concern involves macro-level implementation barriers. These include the economic and logistical costs of upgrading hardware and software, workforce training, lack of standardized tooling, and inconsistent regulatory guidance across jurisdictions. Such issues are particularly acute for small and medium-sized enterprises (SMEs), which often lack the capital and expertise to undertake large-scale cryptographic transitions. According to [51], U.S. federal agencies alone are projected to spend over $7 billion on PQC transition efforts by 2035 excluding national security systems. The [52] compares the scale of this transition to Y2K preparedness, reinforcing the need for cost–benefit frameworks that help policymakers and organizations assess return on investment based on risk exposure and infrastructure readiness.

To synthesize these findings, we introduce a conceptual framework (Fig. 7) that maps emerging quantum threats such as those posed by Shor's and Grover's algorithms to their respective countermeasures, including PQC, QKD, and hybrid cryptographic models. The framework also identifies critical research gaps in implementation, standardization, and stakeholder readiness, offering a roadmap for future research and institutional planning.

Bridging these gaps will require cross-sector collaboration, especially between quantum physicists, cryptographers, and cybersecurity experts. Establishing interdisciplinary testbeds and pilot projects within national infrastructure initiatives supported by policies like the U.S. CHIPS Act and the EU Digital Europe Programme could accelerate real-world validation. These initiatives will be crucial for ensuring that PQC solutions evolve from theoretical promise to operational security at scale.

4 Discussion

4.1 Interpretation of findings

This review highlights both the accelerating progress and persistent challenges associated with preparing cybersecurity systems for the quantum era. The findings reveal that sector-specific approaches dominate the landscape, with critical infrastructure sectors including electoral systems, industrial controls, defence, and finance each demonstrating distinct vulnerabilities. Studies like [24, 33] underscore how legacy technologies, often lacking in agility and upgradability, complicate efforts to implement PQC measures. This is further echoed in defence-related research [40] and secure communication protocols [32], where emerging quantum threats target encrypted data transit points.

The shift toward post-quantum solutions is well underway, particularly in cryptographic innovations such as lattice-based, multivariate, and hybrid schemes. Notably, CRYSTALS-Kyber and CRYSTALS-Dilithium selected by NIST demonstrate promise in terms of performance, compatibility, and standardization potential. Early adoption across sectors adds momentum: [53, 54] are piloting quantum-secure networks, while regulatory bodies like NIST and the European Commission are developing structured migration guidelines.

Despite progress, scalability remains a critical barrier, particularly in low-resource systems such as IoT. Studies by [26, 30, 39] explore lattice-based cryptography and hybrid PQC-QKD models in constrained environments, highlighting gains in performance but also exposing challenges related to key size, message length, and processing overhead. Feasibility is especially limited in real-world deployments outside laboratory conditions [34].

A key insight is the need for integration and algorithm agility. While QKD offers near-perfect security, it requires specialized infrastructure, limiting adoption. Lattice-based schemes, compatible with classical networks, offer a more immediate solution, though they still require rigorous security audits and adaptation for diverse platforms [55]. Cost remains another major obstacle: [51] estimates over $7 billion in U.S. federal PQC transition costs by 2035, echoing comparisons with Y2K-scale transitions [52]. These figures underscore the necessity of cost–benefit models to guide prioritization and policy.

This review also emphasizes the importance of interdisciplinary and cross-sector collaboration, which remains limited. Research linking PQC with AI-enabled cybersecurity such as machine learning/deep learning (ML/DL)-enhanced threat detection or blockchain-based identity systems remains underexplored, despite its potential for creating adaptive and scalable defence layers [43, 56]. The study [15] proposed a migration framework, but questions regarding operational feasibility, cross-platform deployment, and stakeholder readiness remain unanswered.

Geographic trends reveal a concentration of published research from Indian institutions, reflecting the region's growing engagement with quantum technologies. However, this imbalance calls attention to the need for globally distributed efforts, particularly in deployment readiness and policy standardization. Leading international organizations such as NIST [57] and ENISA [58] are paving strategic pathways, but broader international participation is needed to avoid asymmetries in adoption, readiness, and compliance.

In summary, while post-quantum solutions are progressing rapidly, this review reveals that real-world implementation is hindered by scalability, infrastructure readiness, economic viability, and interdisciplinary alignment. Bridging these gaps requires investment in testing environments, collaborative frameworks, and adaptive policy mechanisms to ensure that PQC transitions are both secure and equitable at a global scale.

4.2 Limitations and future work

While this review offers structured insights into the intersection of QC and cybersecurity, several limitations must be acknowledged that affect the breadth, depth, and generalizability of its findings.

Firstly, time constraints imposed by the assignment-based nature of this review significantly limited the scope of the analysis. The need to balance feasibility with comprehensiveness necessitated the application of strict inclusion and exclusion criteria, which, while ensuring methodological consistency, may have resulted in the omission of relevant studies. This constrained both the volume and thematic diversity of the included literature, potentially narrowing the spectrum of perspectives and insights reflected in the findings.

A further limitation lies in the early developmental stage of PQC. Although many studies present promising theoretical frameworks, only a small subset have been evaluated under real-world conditions. Field experiments by major institutions (e.g., Google's hybrid TLS deployments) have revealed that PQC integration faces practical obstacles related to latency, memory overhead, and infrastructure compatibility [59]. This lack of large-scale, empirical validation limits the current ability to assess the real-world viability of proposed solutions.

The review also exhibits a degree of publication bias due to its reliance on peer-reviewed journal articles and conference papers as primary data sources. While this ensures academic rigor, it excludes grey literature, such as government reports, white papers, and technical standards drafts, which may contain valuable insights into industry practices, regulatory developments, and applied case studies [60].

Finally, the rapidly evolving nature of QC presents an inherent challenge. Advances in quantum hardware, cryptographic design, and standardization occur frequently, meaning that some findings particularly those grounded in theoretical projections may quickly become outdated or require re-evaluation.

In summary, while this review contributes meaningfully to ongoing discourse, addressing these limitations in future studies through broader literature inclusion, interdisciplinary collaboration, and real-world testing will be essential for developing truly scalable, secure, and future-proof quantum-resistant cybersecurity solutions.

5 Conclusion

This systematic review has examined the intersection of QC and cybersecurity, providing a structured synthesis of emerging threats, proposed solutions, and critical research gaps from 2019 to 2024. The review reaffirms that QC represents a transformational yet disruptive force, with the potential to compromise widely used cryptographic systems and pose serious risks to digital infrastructures.

Central to these concerns is the vulnerability of traditional encryption methods, particularly RSA and AES, to quantum algorithms such as Shor's and Grover's. In response, the cybersecurity community has developed a growing body of PQC solutions, particularly lattice-based, hybrid, and QKD models. While these solutions show strong theoretical promise and are gaining traction through initiatives such as the NIST standardization process, real-world deployment remains constrained by scalability issues, cost barriers, and integration complexity.

A significant contribution of this review lies in its identification of persistent research and implementation gaps. These include the lack of large-scale empirical testing, limited interdisciplinary collaboration especially between PQC researchers and AI/ML experts and insufficient economic analysis of migration costs. The review emphasizes the need for more adaptive frameworks, robust pilot programs, and collaborative policy-making to guide the global transition to quantum-resilient infrastructures.

Methodologically, this review adhered to the PRISMA framework, ensuring a transparent and reproducible selection process. By focusing on peer-reviewed journal articles and conference papers, academic rigor was maintained. However, the exclusion of grey literature may have limited insight into industry practices and real-world deployments. A follow-up review is already planned to include industry reports, preprints, and technical standards, aiming to capture a broader, practice-informed perspective and reduce potential publication bias.

In conclusion, as QC continues to evolve, the need for scalable, secure, and implementable PQC solutions becomes increasingly urgent. This review calls for accelerated research, cross-disciplinary partnerships, and policy-level engagement to close the gap between cryptographic innovation and operational deployment. Policymakers are encouraged to support large-scale pilot initiatives, while practitioners should begin risk assessments and crypto-agility planning, including exploration of hybrid frameworks. These collective actions will be critical to achieving a smooth and secure transition to the quantum-safe era of cybersecurity.

Abbreviations

AES	Advanced encryption stan`dard
AI	Artificial intelligence
DL	Deep learning
IoT	Internet of Things
KEM	Key encapsulation mechanism
ML	Machine learning
NIST	National institute of standards and technology
PQC	Post-quantum cryptography
PRISMA	Preferred reporting items for systematic reviews and meta-analyses
QKD	Quantum key distribution
RSA	Rivest–Shamir–Adleman encryption
SNDL	Store-now-decrypt-later

Acknowledgements
We extend our gratitude to our institute for their unwavering moral support.

Author contributions
Conceptualization: F.B-d, F.A; Writing Original Draft: F.B-d; Software: F.B-d; Investigation: F.B-d, F.A; Validation: F.B-d, F.A; Visualization: F.B-d; Supervision: F.A.

Funding
This research received no external funding.

Availability of data and materials
No datasets were generated or analysed during the current study.

Declarations

Ethics approval, consent to participate, and Consent to Publish
Not applicable. No humanor animal research was conducted; all data were from previously published sources

Competing interests
The authors declare no competing interests.

Received: 12 March 2025 / Accepted: 12 June 2025
Published online: 29 September 2025

References

1. Li W, Yin Z, Li X, Ma D, Yi S, Zhang Z, et al. A hybrid quantum computing pipeline for real world drug discovery. Sci Rep. 2024;14:16942.
2. Alshammari N, Shahzadi S, Alanazi SA, Naseem S, Anwar M, Alruwaili M, et al. Security monitoring and management for the network services in the orchestration of SDN-NFV environment using machine learning techniques. Comput Syst Sci Eng. 2024;48:363–94.
3. Jaques S, Naehrig M, Roetteler M, Virdia F (2020) Implementing Grover oracles for quantum key search on AES and LowMC. In: Advances in cryptology–EUROCRYPT 2020: 39th annual international conference on the theory and applications of cryptographic techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part II 30, pp 280–310
4. Bhatia V, Ramkumar K (2020) An efficient quantum computing technique for cracking RSA using Shor's algorithm. In: 2020 IEEE 5th international conference on computing communication and automation (ICCCA), pp 89–94
5. Grimes RA. Cryptography apocalypse: preparing for the day when quantum computing breaks today's crypto. New York: Wiley; 2019.
6. Raheman F. The future of cybersecurity in the age of quantum computers. Future Internet. 2022;14:335.
7. Cano Aguilera A, Rubio Garcia C, Lawo D, Imaña JL, Tafur Monroy I, Vegas Olmos JJ. In-line rate encrypted links using pre-shared post-quantum keys and DPUs. Sci Rep. 2024;14:21227.
8. Dimitrov V, Vigneri L, Attias V. Fast generation of RSA keys using smooth integers. IEEE Trans Comput. 2021;71:1575–85.
9. Kumar M, Yadav V, Yadav SP. Advance comprehensive analysis for Zigbee network-based IoT system security. Discover Comput. 2024;27:22.
10. Somsuk K. The improved estimation of the least upper bound to search for RSA's private key. KSII Trans Internet Inf Syst (TIIS). 2022;16:2074–93.
11. Liu T (2020) The applications and challenges of quantum teleportation. In: Journal of physics: conference series, p 012089
12. Claudino D. The basics of quantum computing for chemists. Int J Quantum Chem. 2022;122: e26990.
13. Wang Z, Zhao Y, Zhong G (2019) Public-key applications in E-commerce. In; Journal of physics: conference series, p 042083
14. Chen J. The future of quantum computer advantage. Am J Comput Math. 2023;13:619–31.
15. Umbrello S. Ethics of quantum technologies: a scoping review. Int J Appl Philos. 2024;20:24. https://doi.org/10.5840/ijap202448201.
16. Joseph D, Misoczki R, Manzano M, Tricot J, Pinuaga FD, Lacombe O, et al. Transitioning organizations to post-quantum cryptography. Nature. 2022;605:237–43.
17. Allgyer W, White T, Youssef TA. Securing the future: A comprehensive review of post-quantum cryptography and emerging algorithms. SoutheastCon. 2024;2024:1282–7.
18. Näther C, Herzinger D, Gazdag S-L, Steghöfer J-P, Daum S, Loebenberger D. Migrating software systems towards post-quantum cryptography–a systematic literature review. IEEE Access. 2024. https://doi.org/10.1109/ACCESS.2024.3450306.
19. Sosnowski M, Wiedner F, Hauser E, Steger L, Schoinianakis D, Gallenmüller S et al (2023) The performance of post-quantum tls 1.3. In; Companion of the 19th international conference on emerging networking experiments and technologies, pp 19–27
20. Guz AN, Rushchitsky JJ. Scopus: a system for the evaluation of scientific journals. Int Appl Mech. 2009;45:351–62.
21. Johnson N, Phillips M. Rayyan for systematic reviews. J Electron Resour Librariansh. 2018;30:46–8.
22. Cicchetti DV. The reliability of peer review for manuscript and grant submissions: a cross-disciplinary investigation. Behav Brain Sci. 1991;14:119–35.
23. Blackburn JL, Hakel MD. An examination of sources of peer-review bias. Psychol Sci. 2006;17:378–82.
24. Rodríguez-Pérez A, Costa N, Finogina T (2024) An electoral exception? Quantum computing-readiness and internet voting. In: JeDEM-eJournal of eDemocracy and Open Government, vol. 16
25. Tiwari A, Chauhan R, Joshi N, Devliyal S, Aluvala S, Kumar A (2024) The quantum threat: implications for data security and the rise of post-quantum cryptography. In: 2024 IEEE 9th international conference for convergence in technology (I2CT), pp 1–7
26. Scientific LL (2024) Enhancing cloud security based on the kyber key encapsulation mechanism. J Theor Appl Inf Technol, 102
27. Yalamuri G, Honnavalli P, Eswaran S. A review of the present cryptographic arsenal to deal with post-quantum threats. Procedia Comput Sci. 2022;215:834–45.
28. Nisha F, Lenin J, Saravanan S, Rohit VR, Selvam P, Rajmohan M (2024) Lattice-based cryptography and NTRU: quantum-resistant encryption algorithms. In: 2024 international conference on emerging systems and intelligent computing (ESIC), pp 509–514
29. Figlarz GR, Hessel FP (2022) Applied post-quantum secure method for IoT devices: a case study for autonomous vehicles communication. In: 2022 IEEE 8th World Forum on Internet of Things (WF-IoT), pp 1–6
30. Kumar M (2022) Post-quantum cryptography Algorithm's standardization and performance analysis. Array. 15: 100242
31. Pabla T, Sultana A (2024) Modular blockchain architecture: securing data with quantum-safe encryption. In: 2024 international conference on quantum communications, networking, and computing (QCNC), pp 198–203
32. Baseri Y, Chouhan V, Hafid A. Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols. Comput Secur. 2024;142:103883.
33. del Moral JO, et al. Cybersecurity in critical infrastructures: a post-quantum cryptography perspective. IEEE Internet of Things J. 2024;11(18):30217–44.
34. Henge SK, Jayaraman G, Sreedevi M, Rajakumar R, Rashid M,. Alshamrani SS et al (2023) Secure keys data distribution based user-storage-transit server authentication process model using mathematical post-quantum cryptography methodology. Netw Heterogeneous Media 18
35. Alam MM, Arora A, Bhatt A, Devliyal S, Aluvala S (2024) Cryptographic algorithms for IoT devices: a quantum analysis. In: 2024 3rd international conference for innovation in technology (INOCON), pp 1–7
36. Hasan KF, Simpson L, Baee MAR, Islam C, Rahman Z, Armstrong W, et al. A framework for migrating to post-quantum cryptography: security dependency analysis and case studies. IEEE Access. 2024;12:23427–50.
37. He A, Lou D, She E, Guo S, Watson H, Weng S, et al. (2023) FIPS compliant quantum secure communication using quantum permutation pad. In: 2023 6th world symposium on communication engineering (WSCE), pp 39–44

38. Jenefa A, Josh F, Taurshia A, Kumar KR, Kowsega S, Naveen E (2023) PQC secure: strategies for defending against quantum threats. In: 2023 2nd international conference on automation, computing and renewable systems (ICACRS), pp 1799–1804
39. Biswas S, et al. Exploring the fusion of lattice-based quantum key distribution for secure Internet of Things communications. IET Quantum Commun. 2024;5:322–39.
40. Çakal K, Özdemir S (2024) Transforming military security: quantum age blockchain architecture for IoBT-PARS. In: 2024 international conference on smart applications, communications and networking (SmartNets), pp 1–6
41. Khorkheli L, Bourne D, Chakravarty V, Abraham S, Satrya GB, Mnaouer AB (2024) Improving OTP authentication with PQC algorithms. In: 2024 global information infrastructure and networking symposium (GIIS), pp 1–6
42. Castiglione A, Esposito JG, Loia V, Nappi M, Pero C, Polsinelli M. Integrating post-quantum cryptography and blockchain to secure low-cost IoT devices. IEEE Trans Ind Inform. 2024. https://doi.org/10.1109/ACCESS.2024.3450306.
43. Yavuz AA, Nouma SE, Hoang T, Earl D, Packard S (2022) Distributed cyber-infrastructures and artificial intelligence in hybrid post-quantum era. In: 2022 IEEE 4th international conference on trust, privacy and security in intelligent systems, and applications (TPS-ISA), pp 29–38
44. Shahzadi S, Ahmad F, Basharat A, Alruwaili M, Alanazi S, Humayun M, et al. Machine learning empowered security management and quality of service provision in SDN-NFV environment. Comput Mater Continua. 2020;66:2723–49.
45. Ud-Din MM, Alshammari N, Alanazi SA, Ahmad F, Naseem S, Khan MS, et al. InteliRank: a four-pronged agent for the intelligent ranking of cloud services based on end-users' feedback. Sensors. 2022;22:4627.
46. Shabbir M, Ahmad F, Shabbir A, Alanazi SA. Cognitively managed multi-level authentication for security using Fuzzy Logic based Quantum Key Distribution. J King Saud Univ Comput Inf Sci. 2022;34:1468–85.
47. Nazir A, He J, Zhu N, Wajahat A, Ma X, Ullah F, et al. Advancing IoT security: a systematic review of machine learning approaches for the detection of IoT botnets. J King Saud Univ Comput Inf Sci. 2023;35: 101820.
48. Nazir A, He J, Zhu N, Wajahat A, Ullah F, Qureshi S, et al. Collaborative threat intelligence: enhancing IoT security through blockchain and machine learning integration. J King Saud Univ Comput Inf Sci. 2024;36: 101939.
49. Wajahat A, He J, Zhu N, Mahmood T, Nazir A, Ullah F, et al. Securing Android IoT devices with GuardDroid transparent and lightweight malware detection. Ain Shams Eng J. 2024;15: 102642.
50. Ahmad F, Kanta K, Shiaeles S, Naeem A, Khalid Z, Mahboob K (2024) Enhancing ATM security management in the post-quantum era with quantum key distribution. In: 2024 IEEE international conference on cyber security and resilience (CSR), pp 329–334
51. Williams BK (2024) The US needs a strategy for the second quantum revolution. Lawfare
52. Moody (2024). Moody's sounds alarm on quantum computing risk, as transition to PQC 'will be long and costly. Available: https://industrialcyber.co/reports/moodys-sounds-alarm-on-quantum-computing-risk-as-transition-to-pqc-will-be-long-and-costly/
53. JPMorgan (2022) JPMorgan establishes quantum-secured, crypto-agile network. Available: https://www.jpmorgan.com/technology/news/firm-establishes-quantum-secured-crypto-agile-network
54. HSBC (2024) HSBC pilots quantum-safe technology for tokenised gold. Available: https://www.hsbc.com/news-and-views/news/media-releases/2024/hsbc-pilots-quantum-safe-technology-for-tokenised-gold
55. Amirkhanova DS, Iavich M, Mamyrbayev O. Lattice-based post-quantum public key encryption scheme using ElGamal's principles. Cryptography. 2024;8:31.
56. Hasan T, Ahmad F, Rizwan M, Alshammari N, Alanazi SA, Hussain I, et al. Edge caching in fog-based sensor networks through deep learning-associated quantum computing framework. Comput Intell Neurosci. 2022;2022:6138434.
57. Chen L, Chen L, Jordan S, Liu Y-K, Moody D, Peralta R et al (2016) Report on post-quantum cryptography vol. 12: US Department of Commerce, National Institute of Standards and Technology…,
58. Beullens W, D'Anvers J-P, Hülsing AT, Lange T, Panny L, de Saint Guilhem C, et al (2021) Post-quantum cryptography: current state and quantum mitigation
59. Bernstein DJ, Lange T. Post-quantum cryptography. Nature. 2017;549:188–94.
60. Thornton A, Lee P. Publication bias in meta-analysis: its causes and consequences. J Clin Epidemiol. 2000;53:207–16.

Publisher's note