INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2026, VOL. 72, NO. 2, PP. 1-9
Manuscript received April 2, 2026; revised April, 2026. doi: 10.24425/ijet.2026.157908

Federated learning and Quantum Computing for cybersecurity in the banking Sector: a systematic review

Jean Marie Vianney Sindayigaya

***Abstract*—The modern banking sector faces growing cybersecurity challenges, demanding collaborative yet privacy-preserving defense mechanisms. Federated Learning (FL) has emerged as a key paradigm for addressing these needs, but the advent of quantum computing threatens its long-term viability. This development introduces a critical duality: the existential threat of quantum capabilities to break classical cryptography and the transformative opportunities offered by Quantum Machine Learning (QML). While research has addressed these aspects separately, a unified analysis that unites them is lacking. This paper presents the first comprehensive systematic review mapping this dualistic landscape. Following PRISMA guidelines, the review synthesizes the current state of research and evaluates the challenges and opportunities at the intersection of FL, quantum computing, and financial cybersecurity. The findings reveal a strong consensus on the urgent need to integrate Post-Quantum Cryptography (PQC) to secure FL frameworks against future threats. Simultaneously, a long-term vision is emerging to leverage QML to enhance threat detection capabilities beyond classical boundaries. A significant trend toward integrated, layered architectures that combine FL, blockchain, and quantum technologies is also identified. This review concludes that the evolution of FL in banking is inextricably linked to quantum advances, demanding a two-pronged proactive strategy: mitigating immediate risks with PQC while strategically investing in R&D for QML.**

***Keywords*—federated learning; quantum computing; cybersecurity; banking; systematic review**

I. Introduction

THE modern banking sector faces an escalating landscape of sophisticated cyber threats, ranging from phishing and malware to novel risks threatening the adoption of digital banking [1]. In response, Federated Learning (FL) has emerged as a promising paradigm, enabling banks to collaboratively train robust AI models for applications like fraud detection without sharing sensitive client data, thus balancing enhanced security with privacy compliance [2]. However, as the world prepares for the next computational revolution, this existing FL paradigm faces an inevitable disruption: the dawn of the quantum computing era. The advent of quantum computing presents a fundamental duality; on one hand, it poses an existential threat capable of breaking the conventional cryptographic systems like RSA and ECC that form the backbone of global digital security [3]. On the other hand, it offers transformational opportunities through Quantum Machine Learning (QML) for financial applications, promising superior accuracy and speed [4].

This strategic duality has catalyzed two parallel yet seldom-connected streams of research. One stream actively explores the integration of quantum principles to enhance FL capabilities, such as employing Quantum Neural Networks (QNNs) within hybrid frameworks to improve fraud detection accuracy [5], aligning with the broader vision of technological convergence for a more efficient fintech ecosystem [6]. Conversely, the urgency of the quantum threat has spurred the development of explicitly quantum-resistant protocols, including lattice-based Quantum-Resistant Federated Learning Protocols (QFLP) [7] and post-quantum secure secret sharing schemes [8]. However, while these studies individually address either the opportunity or the threat, the existing literature remains fragmented. A comprehensive systematic review that maps both sides of this duality, analyzes their combined challenges, and charts a coherent roadmap for FL in the quantum era is conspicuously absent.

To address this critical gap, this paper presents the first comprehensive systematic review aimed at synthesizing these disparate research streams into a unified, coherent landscape. By adopting a systematic review methodology—ideal for mapping nascent, complex, and interdisciplinary research fields [9], [10]—this study provides a rigorous foundation for future discourse, moving beyond the ad-hoc nature of current discussions [11]. Specifically, this research seeks to answer the following fundamental questions:

- (RQ1) How can quantum computing applications enhance the capabilities of FL systems for cybersecurity in the banking sector?
- (RQ2) What are the fundamental technical, security, and operational threats and challenges posed by quantum computing to FL implementations?
- (RQ3) What are the future research and development directions for building quantum-resistant and quantum-enhanced FL frameworks for the banking sector?

The remainder of this article is organized as follows. Section 2 establishes the theoretical foundation for this review, detailing the core concepts of Federated Learning in the financial sector and framing the quantum revolution as a 'double-edged sword'

Author is with Warsaw University of Technology, Poland (corresponding author e-mail: jean_marie_vianney.sindayigaya.dokt@pw.edu.pl).

© The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0, https://creativecommons.org/licenses/by/4.0/), which permits use, distribution, and reproduction in any medium, provided that the Article is properly cited.

of cryptographic threats and machine learning opportunities. Subsequently, Section 3 out-lines the systematic review methodology, detailing the PRISMA guidelines, search strategy, and the inclusion/exclusion criteria used to ensure a rigorous and transparent selection of studies. Section 4 presents the core findings of the analysis, mapping the research landscape according to the dual themes of the 'Quantum Threat' and the 'Quantum Opportunity,' alongside the emergent meta-theme of convergence towards integrated frameworks. Following this, Section 5 provides an in-depth discussion of these findings, interpreting their strategic implications for the financial industry, acknowledging the study's strengths and limitations, and proposing concrete directions for future research. Finally, Section 6 concludes the paper by summarizing its key insights and reinforcing the strategic importance of developing integrated, quantum-ready frameworks for the future of financial cybersecurity.

II. Literature Review and Theoretical Foundations

A. Federated Learning in the Financial Sector: A Privacy-Preserving Paradigm

The modern financial services sector, particularly banking, faces a fundamental dilemma between the need for data collaboration for innovation and stringent privacy mandates. Traditional, centralized approaches to building machine learning (ML) models now face significant privacy and data security challenges [12], an issue exacerbated by global data protection regulations such as the General Data Protection Regulation (GDPR) [13]. In response, Federated Learning (FL) has emerged as a promising paradigm, introducing a decentralized architecture in which multiple entities, such as banks, can collaboratively train models without exchanging raw data [14]. In an FL framework, each institution trains models locally on its own data and only shares model updates (e.g., gradients or weights) with a central server. This mechanism ensures that sensitive customer data never leaves each institution's local environment [12], [14]. Thus, FL effectively addresses the conflict between data-driven innovation and regulatory compliance, enabling the development of advanced AI models while fundamentally preserving data privacy.

The utility of this paradigm has been demonstrated in numerous practical applications in the banking sector. One of the most prominent application areas is fraud detection, where FL enables multiple banks to collaboratively train more sophisticated credit card fraud detection models collaboratively, thus identifying new anomalous patterns without having to share highly sensitive customer transaction data [15]. Furthermore, FL is widely applied in credit risk assessment and credit scoring, enabling financial institutions to build more accurate and reliable credit scoring models by leveraging insights from larger, more diverse datasets [16], [17]. Another crucial area is Anti-Money Laundering (AML), where FL can enhance the ability to detect complex and distributed money laundering networks across institutions. This task is challenging to perform with isolated systems [18]. Collectively, these applications demonstrate that FL provides a real solution for banks to overcome data silos, resulting in more robust, accurate analytical models for risk mitigation and compliance without compromising data privacy and security.

While FL offers an elegant solution, this paradigm is not without inherent operational and technical challenges [19]. The first fundamental challenge is data heterogeneity, or non-independent and identically distributed (non-IID) data, in which the distribution of data across participants can vary significantly, leading to degradation of the global model's performance [20]. Second, communication overhead is a significant practical concern, as the iterative process of sending model updates can consume significant network resources and be energy-intensive, thus demanding efficient resource allocation mechanisms [21]. Finally, from a security perspective, the decentralized nature of FL also introduces new attack vectors, making the model vulnerable to adversarial attacks in which malicious participants may attempt to undermine the integrity of the global model [22]. These classic challenges underscore that, even before considering quantum disruption, FL is a field that requires careful design for successful implementation in critical environments such as banking.

B. The Quantum Revolution: A Double-Edged Sword for Finance

1) The Threat: Post-Quantum Cryptography (PQC) as a Necessity

The advent of quantum computers relevant to cryptography introduces a funda-mental, and potentially existential, threat to the cryptographic security underpinning the global financial system [23]. This threat stems from the ability of quantum algorithms, particularly Shor's Algorithm, to solve the mathematical problems that underpin modern public-key cryptography [24], [25]. Currently dominant cryptographic systems, such as RSA and Elliptic Curve Cryptography (ECC), rely on the classical computational difficulty of factoring huge prime numbers. However, Shor's Algorithm can solve this problem in polynomial time, theoretically making them vulnerable to breach. The consequences are not merely theoretical; they represent a fundamental shift in the security assumptions that protect everything from banking transactions and customer data communications to the integrity of capital markets. Furthermore, this threat is retroactive, giving rise to a "harvest now, decrypt later" scenario where encrypted data stolen today could be de-crypted in the future when a capable quantum computer becomes available.

In response to these threats, the global cryptography community is proactively developing a solution known as Post-Quantum Cryptography (PQC). PQC refers to a class of cryptographic algorithms designed to be secure against attacks by both classical and quantum computers, as they are based on mathematical problems believed to be difficult to solve even by quantum computers [16]. The effort to standardize these algorithms is being led globally by the National Institute of Standards and Technology (NIST) in the United States [26], [27], [28]. Through a rigorous multi-round competition process, NIST has begun finalizing and recommending candidate PQC algorithms for wide-scale adoption. This standardization process sends a clear signal to the industry, including the finance and accounting sectors, about the urgency of preparing for the migration. This transition is not simply a technical update, but

a strategic shift that requires careful planning, the development of cryptographic agility, and the creation of a comprehensive roadmap to ensure the security of payment systems and financial data in the future [23], [28]. Therefore, adopting a PQC framework is no longer an option, but rather a strategic imperative to maintain integrity and trust in financial infrastructure in the post-quantum era.

2) The Threat: Post-Quantum Cryptography (PQC) as a Necessity

On the other side of the cryptographic threat, quantum computing presents trans-formative opportunities through the field of Quantum Machine Learning (QML), which is seen as one of the most promising future applications [29]. While classical machine learning has been successful, its approaches are often very resource intensive [30]. QML aims to overcome these limitations by leveraging quantum principles, such as super-position and entanglement, to process information in fundamentally different ways. One key mechanism is quantum feature mapping, in which classical data is mapped into a high-dimensional Hilbert space using quantum circuits. This process has the potential to increase feature separability and enable algorithms to discover patterns that are difficult or impossible to access with classical methods [31]. The result is a potential quantum advantage, with significant computational speed-ups and increased predictive accuracy compared to traditional models. Therefore, QML represents a paradigm shift from simply optimizing classical algorithms to designing algorithms that inherently harness the power of quantum computing.

The theoretical potential of QML is actively explored to solve the most challenging computational problems in the financial sector. One of the most researched domains is portfolio optimization, where algorithms such as the Quantum Support Vector Machine (QSVM) [32] and the Quantum Approximate Optimization Algorithm (QAOA) [33] have been proposed to find optimal asset allocations efficiently. This task is inherently complex and is a prime target for quantum acceleration [34], [35]. Furthermore, QML shows great potential in risk management and derivatives pricing. Research has shown that Quantum Neural Networks (QNNs) can be used to compute important risk measures, such as 'Greeks' (e.g., delta and gamma) [24], and that techniques such as Quantum Amplitude Estimation can accelerate Monte Carlo simulations for risk analysis [25]. Overall, these applications highlight the primary goal of QML in finance: harnessing the power of quantum computing to gain an advantage in speed or accuracy, thereby enabling better decision-making in dynamic and complex market environments [32], [36].

3) The Threat: Post-Quantum Cryptography (PQC) as a Necessity

From the previous discussion, the existing literature broadly addresses Federated Learning (FL) and the quantum computing revolution as two parallel domains. On the one hand, there is extensive research on FL applications in the financial sector. On the other hand, systematic reviews on quantum finance have also been conducted, but often without considering distributed learning paradigms such as FL [37]. Nevertheless, pioneering research is emerging to bridge this gap, forming an interdisciplinary field known as Quantum Federated Learning (QFL) [38], [39], [40]. These early studies have begun to explore how FL can be integrated with quantum cryptography for specific purposes, such as the scalability of Quantum Key Distribution (QKD) [41], or how QFL frameworks can be applied across various industries, including finance [36].

However, a significant theoretical gap remains. The existing literature tends to focus either on threats or opportunities or on specific technical implementations, while a comprehensive, integrated analysis is lacking. No systematic review has specifically mapped the landscape of this duality in the banking sector: namely, the urgent need to secure existing FL architectures with Post-Quantum Cryptography (PQC) while simultaneously exploring the transformative opportunities of Quantum Machine Learning (QML) to enhance their capabilities. This paper aims to fill this gap by presenting the first synthesis that brings together both sides of this quantum double-edged sword, providing an integrated view and strategic roadmap for the banking industry.

III. METHODOLOGY

A. Review Guideline

This systematic review was designed and reported in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines [42]. The use of this structured framework is essential to ensure methodological transparency, rigor, and replicability, as well as to minimize potential bias in the study se-lection and synthesis process.

B. Search Strategy

The literature search process aims to identify high-quality articles relevant to the synergistic intersection between Federated Learning, quantum computing, and financial cybersecurity.

1) Information Sources

To ensure a comprehensive search, four primary sources were used: ACM Digital Library, IEEE Xplore, Scopus, and arXiv. The first three databases were chosen for their extensive coverage of peer-reviewed literature. At the same time, arXiv was added to capture the latest preprints that are highly relevant in this rapidly evolving field.

2) Search String

A systematic search strategy was developed using precise keyword combinations to capture relevant literature. The primary search query incorporated terminology from three core concepts as follows: ("Federated Learning" OR "Decentralized Machine Learning" OR "Collaborative Learning") AND ("Quantum Computing" OR "Quantum Machine Learning" OR "Post-Quantum Cryptography" OR "Quantum-Resistant") AND ("Banking" OR "Financial Services" OR "Fintech" OR "Cybersecurity"). Boolean operators (AND, OR) were consistently used to combine these conceptual pillars, ensuring the identification of studies that specifically addressed their intersection.

3) Search Limitations

To ensure relevance and maintain the review's focus, several limitations were ap-plied during the search process. The publication timeframe was limited to articles published between

January 2022 and November 2025, a period chosen to capture the most recent developments in these rapidly evolving fields. The search was narrowed to relevant subject areas, including Computer Science, Engineering, Mathematics, and Quantitative Finance. Furthermore, only articles written in English and representing journal articles or conference papers were considered. Non-primary publications such as literature reviews, editorials, and abstracts without full text were systematically excluded from the initial search process.

C. Selection Criteria

After the automated search is complete, the process proceeds to a two-stage manual screening. The first stage involves reviewing titles and abstracts, followed by an in-depth analysis of the full text of potentially relevant articles, all guided by predefined inclusion and exclusion criteria.

1) Inclusion Criteria

A study was included in the final analysis if it met all of the following criteria:

1. The study type was a primary research article presenting original findings.
2. The study's primary focus was on the intersection of Federated Learning and Quantum Computing in the context of finance or cybersecurity.
3. The article had full text accessible to researchers.

2) Exclusion Criteria

A study was excluded if it was any of the following:

1. Articles that fell into the category of literature reviews, surveys, or editorials.
2. Studies with application domains that fell outside the scope of finance or cybersecurity.
3. Articles for which the full text was inaccessible.

D. Study Selection and Data Extraction Process

The study selection process followed the PRISMA 2020 workflow summarized in Figure 1. The initial search across four sources yielded 64 articles. After removing four duplicates, the remaining 60 unique articles were screened based on title and abstract. At this stage, 56 articles were excluded due to irrelevance. From four potentially relevant articles, the full texts were successfully accessed. These four articles were then fully evaluated for eligibility, and none were excluded at this stage, as all met the inclusion criteria. Thus, a final total of four studies were included in the qualitative synthesis.

For each selected study, data were systematically extracted using a predefined template. Key data points collected included: bibliographic information, research focus, proposed architecture, application domain, identified challenges, and future research directions. The extracted data were then thematically synthesized to identify emerging patterns and core themes across the included studies.

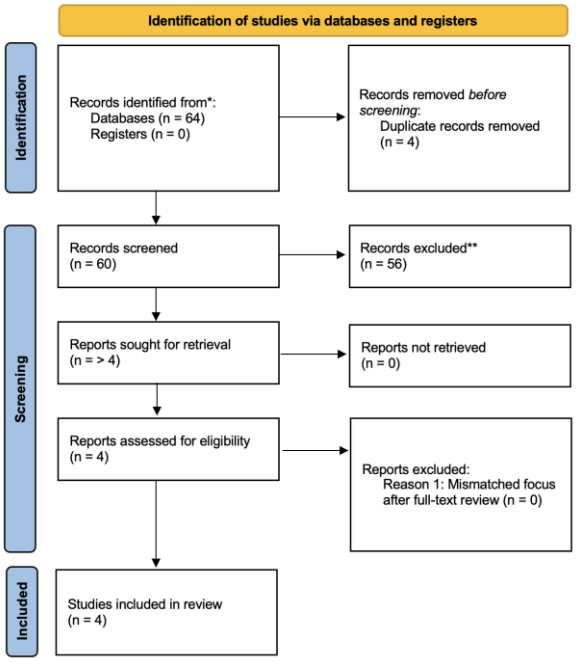

Fig 1. PRISMA 2020 flow diagram for the study selection process.

IV. Results

A. Overview of Included Studies

The qualitative analysis in this systematic review is based on four studies that successfully passed all selection stages. These four studies, published between 2024 and 2025, reflect the nascent nature and rapid development of this interdisciplinary field. All four are primary research articles proposing new frameworks or methodologies that substantively address the intersection of Federated Learning (FL) and quantum computing, with applications in the financial sector or cybersecurity. To provide a clear overview, a summary of each included study, including its primary focus, methodology, and relevant key findings, is presented in Table I.

TABLE I
SUMMARY OF STUDIES INCLUDED IN THE SYSTEMATIC REVIEW

References	Main Focus	Methodology	Relevant Key Findings
[43]	Proposes a privacy-preserving and collusion-resistant FL framework (MKHA-PPFL), with special emphasis on resistance to quantum computing attacks.	Cryptographic Framework Proposal	Demonstrates the integration of Post-Quantum Cryptography (PQC) into a multi-key homomorphic aggregation scheme to secure FL, thereby making it resilient to future quantum threats.
[44]	Proposes a Quantum Federated Neural Network (QFNN-FFD) framework specifically designed for financial fraud detection.	Hybrid Framework Proposal (QML+FL) with Experimental Validation	Shows that combining QML and FL can significantly improve accuracy (precision > 95%) and robustness in

			financial fraud detection tasks, even in environments with quantum noise.
[45]	Analyzing Denial of Service (DoS) attacks and their countermeasures strategies in the context of AI and the Post-Quantum (PQ) era, with a special investigation on collaborative frameworks using federated learning.	Conceptual Analysis and Prospective Review	Identifies that a distributed counter-DoS framework using FL is a promising approach and highlights the importance of considering Post-Quantum (PQ) security inherently in system design.
[46]	Proposes an integrated framework to improve the efficiency, security, and privacy of Quantum Neural Networks (QNNs) in the NISQ era, where Quantum Federated Learning (QFL) is adopted as the core component for privacy.	Integrated Framework Proposal	Affirming that QFL is a fundamental component to enable reliable and privacy-preserving QNNs implementation in the real world, particularly for applications in finance, healthcare, and cybersecurity.

B. Thematic Analysis

A thorough analysis of the four included studies reveals two dominant themes that collectively reflect the dualistic nature of the interaction between quantum computing and Federated Learning. These themes directly address the research question of the threats and opportunities arising from the convergence of these two technologies. The first theme focuses on the defensive aspect, namely, how to secure FL systems against future quantum computing threats. The second theme explores the offensive aspect, or opportunities, namely, leveraging the power of quantum computing to enhance the capabilities and performance of the FL framework itself. In addition to these two primary themes, a significant meta-theme was identified, highlighting the shifting research trend toward integrated, holistic architectures. The following subsections will elaborate on each of these themes in more detail.

1) Theme 1: The Quantum Threat: The Imperative for Post-Quantum Security in FL

Addressing this challenge, the included literature demonstrates a proactive shift from simply recognizing threats to engineering concrete solutions. Rather than waiting for threats to materialize, researchers have begun integrating Post-Quantum Cryptography (PQC) directly into the design of FL frameworks. The most prominent example of this trend is the proposal of an FL framework (MKHA-PPFL) that explicitly guarantees "resistance to quantum computational attacks" [43]. This achievement is realized through the construction of a multi-key homomorphic aggregation scheme on top of a lattice-based cryptographic foundation, which is believed to be secure against quantum attacks. This trend underscores an important consensus: to ensure the long-term viability and security of FL systems, especially in critical domains such as finance, future architectures must be designed with "quantum-readiness" assumptions from the outset.

2) Theme 2: The Quantum Opportunity: Enhancing FL Performance with QML

In contrast to the threat theme, a second prominent theme is the opportunity to proactively harness the power of quantum computing to improve the performance of Federated Learning (FL). This theme centers on the development of Quantum Federated Learning (QFL), a hybrid paradigm in which Quantum Machine Learning (QML) algorithms, specifically Quantum Neural Networks (QNNs), are integrated as local models within an FL framework. This approach aims not only to secure FL but also to improve it fundamentally. One of the most concrete examples of this approach is the development of the Quantum Federated Neural Network for Financial Fraud Detection (QFNN-FFD) [44]. This proposed framework not only theoretically combines both technologies but also experimentally demonstrates that QFL models achieve superior performance, with precision above 95% and exceptional robustness in financial fraud detection tasks, even under quantum noise.

The importance of this integration is further reinforced by positioning QFL as a fundamental component for facilitating "privacy-preserving collaborative training" and laying "the foundation for robust quantum machine learning applications" in critical sectors such as finance and cybersecurity [46]. This positioning suggests that QFL is not merely an academic experiment but a crucial step towards making QNNs applicable in the real world. Collectively, these findings demonstrate that quantum opportunities in the context of FL extend beyond computational acceleration to include increased accuracy, robustness to noise, and the ability to solve more complex problems, all of which are crucial capabilities for future financial applications.

3) Meta-Theme: A Convergence Towards Integrated Frameworks

Beyond the specific themes of threats and opportunities, a collective analysis of the four included studies reveals a more fundamental meta-theme: a clear shift from the exploration of isolated components to the design of integrated, holistic frameworks. Every selected paper, without exception, proposes not a single algorithm, but rather a multi-component architecture designed to address multiple challenges simultaneously. For example, one proposed architecture integrates homomorphic cryptography, federated learning, and post-quantum security into a single, unified system [43]. Similarly, a bridge between Quantum Machine Learning and Federated Learning is explicitly built to create a practical QFL

solution [44], [46]. In fact, conceptual studies not only address FL but also investigate its synergy with blockchain to build collaborative cyber-defense frameworks [45].

This trend indicates a level of maturity in this research field. Researchers are no longer simply asking "can we do it?", but "how do we build a complete, secure, and efficient system for real-world applications?" This convergence suggests that future solutions in the financial sector will not come from a single technology, but rather from the intelligent orchestration of distributed learning, advanced cryptography (both classical and quantum), and robust system architecture. Thus, this meta-theme asserts that the future of FL- and quantum-enabled financial cybersecurity lies in the design of fundamentally integrated systems.

V. Discussion

A. Summary of Principal Findings

The thematic analysis conducted in the previous chapter clearly identified two principal, complementary themes, reflecting the dualistic nature of quantum computing integration into the Federated Learning (FL) ecosystem. The first theme is defensive posture, highlighting the growing awareness of the inherent vulnerability of FL architectures to future quantum computing threats. This awareness drives the urgent need to integrate Post-Quantum Cryptography (PQC) to ensure long-term resilience and security. The second theme, in contrast, is offensive opportunities, exploring the potential to proactively harness the power of quantum computing, particularly through Quantum Machine Learning (QML), to enhance FL capabilities and performance in complex tasks such as financial fraud detection. These two themes collectively illustrate a fundamental dualism: the threats and opportunities facing the financial sector. Beyond these two major themes, a significant meta-theme also emerged: the convergence of research toward the design of unified frameworks. These findings demonstrate that the field is moving be-yond isolated algorithms toward holistic, multi-component system architectures. These findings, which will be further interpreted in the following sub-chapters, provide a comprehensive picture of the strategic landscape that financial industry stakeholders must navigate.

B. Interpretation and Strategic Implications

The findings presented in section 4 not only map the current research landscape but also have profound strategic implications for the future direction of the financial and technology sectors. The following discussion will interpret these findings within a broader context.

1) Navigating Quantum Duality: A Strategic Dilemma for the Financial Sector

This systematic review confirms that Federated Learning (FL) has been established as a critical paradigm for addressing data privacy challenges across various domains, including finance [47]. However, the researchers' key findings reveal that the advent of the quantum era fundamentally alters this strategic calculus. The identified duality between threats and opportunities is not merely a conceptual observation, but a real strategic dilemma that financial institutions must now confront.

This reality is reinforced by a bibliometric analysis [48], which quantitatively demonstrates that the intersection of Quantum Computing, AI, and Financial Risk is a rapidly evolving area of technological disruption. The analysis underscores that financial institutions must be aware of the "potential weaknesses and issues" arising from these transformative technologies. Therefore, financial institutions can no longer focus solely on adopting FL for privacy. They must simultaneously: (1) defend by planning a migration to Post-Quantum Cryptography (PQC) to secure their existing FL infrastructure, and (2) attack by investing in Quantum Machine Learning (QML) research and development to unlock future competitive advantages. The implication is clear: the technology roadmap for financial institutions must include a dual quantum strategy that balances short-term risk mitigation with long-term innovation.

2) Paradigm Shift Toward Integrated Systems: Beyond Single Algorithms

The meta-theme identified by the researchers, namely the shift toward integrated frameworks, signals a significant level of maturity in this research field. This principle resonates strongly with findings in the cybersecurity literature, where greater integration of information systems has been found to encourage, rather than reduce, investment in security [49]. The study theorized that while integration reduces the number of points of vulnerability, the remaining points become much more critical, thereby justifying greater, more focused security investment.

This analogy is highly relevant to the researchers' findings. The movement from single algorithms to holistic frameworks (such as FL + QML, or FL + PQC) demonstrates that researchers recognize that complex problems in the financial sector cannot be solved with isolated solutions. A fraud detection system, for example, requires not only accurate predictive models (QML opportunities), but also fundamentally secure communication channels (PQC threats) and privacy-preserving architectures (FL). The implication is that the era of stand-alone algorithms is over. The future of security and efficiency in the financial sector lies in the ability to design, implement, and manage integrated, multi-technology system architectures, which demands interdisciplinary collaboration be-tween cybersecurity experts, data scientists, and quantum physicists.

3) Strengths and Limitations of the Review

To present these findings in a transparent context, it is important to acknowledge the limitations inherent in this systematic review critically. The most important limitation is the small number of final studies, only four articles. While this limits the generalizability of the findings, the small sample size strongly underscores the authors' central argument: that the field is still in its infancy and that this review fills a significant research gap. Furthermore, there is the potential for publication bias. Significant research and development at the intersection of FL and quantum computing likely occurs internally within large financial institutions or technology companies, with results often not published in the academic literature due to proprietary or confidentiality concerns. Finally, the pace of development in this field is extremely rapid. Consequently, this review is a snapshot of the research landscape at a specific point in time, where new developments emerging after the researchers' research period may alter some aspects of the findings.

Nevertheless, these limitations do not diminish the fundamental strength of this review. Its primary strength lies in

its originality and scope. To the authors' knowledge, this is one of the first systematic reviews to specifically synthesize the dualism of threats (via PQC) and opportunities (via QML) of quantum computing in the context of Federated Learning for the financial sector. By mapping this dualistic landscape, this study provides a coherent synthesis of previously fragmented research streams. Furthermore, its methodological strength cannot be overstated. The use of rigorous PRISMA guidelines ensures that the study selection process is transparent, replicable, and systematic, significantly reducing the risk of bias and enhancing the credibility and validity of the findings. This combination of unique thematic contributions and a strong methodological foundation makes this review a solid foundation for identifying the most pressing future research directions.

C. Future Research Directions

Based on the identified findings and limitations, this systematic review opens up several concrete research avenues crucial for advancing this field from theoretical exploration to practical implementation. The most pressing future research direction is the need for additional primary research. The review highlights the scarcity of case studies and experimental implementations, suggesting that future research should focus on applying Quantum Federated Learning (QFL) frameworks to real-world financial problems to validate their theoretical advantages. While such experimental approaches, which apply quantum computing to practical financial problems, have begun to be explored on a small scale, their implementation in an integrated QFL context remains very limited [50], [51]. Furthermore, as more implementations emerge, the need for systematic benchmarking studies becomes crucial. Future research should develop and implement standard methodologies for conducting fair performance comparisons between various proposed QFL architectures, in line with calls for better standardization and taxonomy in this field [52].

Furthermore, a significant research area is the development of integrated hybrid frameworks. Rather than treating Post-Quantum Defense (PQC) and performance enhancement through Quantum Machine Learning (QML) as separate entities, future re-search should design architectures that explicitly combine them into a single, coherent solution, taking into account emerging cryptographic roadmaps and standards [53]. Finally, practical challenges regarding scalability and economic feasibility need to be addressed. Research should move from proof-of-concept to analyzing the challenges of deploying these solutions at scale. This includes in-depth investigations into cost-benefit analysis, computational scalability, and, most importantly, organizational readiness to adopt such a transformative technology. Recent empirical data has shown that this readiness is a substantial challenge across various critical infrastructure sectors, including finance [54]. Investigating these research directions collectively will be crucial to maturing the field of QFL and paving the way for its secure and efficient adoption in the financial sector.

VI. CONCLUSION

Overall, this systematic review confirms that the convergence of Federated Learning (FL) and quantum computing will fundamentally change the cybersecurity and innovation landscape in the banking sector. This research maps this crucial intersection, confirming that the quantum era introduces a new layer of complexity that fundamentally alters the calculation of risks and opportunities. The core findings emerging from the analysis reveal an apparent duality. On the one hand, there is an urgent, consensus-driven need to strengthen existing FL architectures with Post-Quantum Cryptography (PQC), a fundamental prerequisite for long-term viability. On the other hand, a promising long-term vision emerges to leverage Quantum Machine Learning (QML) to enhance the threat detection capabilities of FL models beyond classical limitations.

These findings are organized into three main themes that inform the following conclusions. First, Quantum Threats confirm that PQC defenses are no longer an option but rather a necessity to ensure the integrity of future FL systems. Second, Quantum Opportunities demonstrates that QML, while still in its infancy, is seen as the next evolutionary step to enhance the intelligence and resilience of financial models. Third, and most significantly, a meta-theme of Convergence towards a Unified Architecture emerges, in which FL, blockchain, and quantum technologies are no longer viewed as isolated components but rather as a synergistic technology stack for intelligence, trust, and security.

Beyond its theoretical contribution in mapping this landscape, this research also provides actionable strategic implications. The proposed roadmap guides industry stakeholders in navigating this quantum duality effectively. Ultimately, the evolution of FL in the banking sector is inextricably linked to quantum advancements, demanding a proactive dual strategy. Financial institutions must simultaneously mitigate existential threats by integrating PQC defenses while strategically investing in research and development to capitalize on QML's transformative opportunities. The integrated framework and findings presented here offer a foundation for both academic inquiry and practical transformation in the era of Quantum Federated Learning.

REFERENCES

[1] Md. Waliullah, M. Z. H. George, M. T. Hasan, M. K. Alam, M. S. K. Munira, and N. A. Siddiqui, "Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review," ArXiv, vol. abs/2503.22710, 2025, [Online]. Available: https://api.semanticscholar.org/CorpusID:277294571

[2] Shreya Gupta, "Federated Learning: Advancing Privacy-Preserving Machine Learning at Scale," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 11, no. 2, pp. 2993–3008, Apr. 2025, https://doi.org/10.32628/cseit25112775

[3] B. Hanafi and M. Ali, "Analyzing the research impact in post quantum cryptography through scientometric evaluation," Discover Computing, vol. 28, no. 1, p. 32, 2025, https://doi.org/10.1007/s10791-025-09507-3

[4] M. Doosti, P. Wallden, C. B. Hamill, R. Hankache, O. T. Brown, and C. Heunen, "A Brief Review of Quantum Machine Learning for Financial Services," ArXiv, vol. abs/2407.12618, 2024, [Online]. Available: https://api.semanticscholar.org/CorpusID:271244438

[5] A. Naidu and B. Student, "The Role of Quantum Neural Networks in Fraud Detection: Opportunities and Challenges." [Online]. Available: www.ijfmr.com

[6] S. Dagur, "AI-Driven Transparency in Fintech Payments: Revolutionizing Trust and Efficiency." [Online]. Available: https://lloydbusinessreview.com

[7] "Quantum-Resistant Federated Learning Protocol with Secure Aggregation for Cross-Border Fraud Detection," International Journal of Computer Applications Technology and Research, Jun. 2025, https://doi.org/10.7753/ijcatr1012.1010

[8] X. Zhang, H. Deng, R. Wu, J. Ren, and Y. Ren, "PQSF: post-quantum secure privacy-preserving federated learning," Sci Rep, vol. 14, no. 1, Dec. 2024, https://doi.org/10.1038/s41598-024-74377-6

[9] D. Javeed, M. S. Saeed, I. Ahmad, M. Adil, P. Kumar, and A. K. M. N. Islam, "Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions," Future Generation Computer Systems, vol. 160, pp. 577–597, Nov. 2024, https://doi.org/10.1016/j.future.2024.06.023

[10] A. Mathur, A. Gupta, and S. K. Das, "When Federated Learning Meets Quantum Computing: Survey and Research Opportunities," ArXiv, vol. abs/2504.08814, 2025, [Online]. Available: https://api.semanticscholar.org/CorpusID:277780858

[11] B. C. Stahl and D. Eke, "The ethics of ChatGPT – Exploring the ethical issues of an emerging technology," Int J Inf Manage, vol. 74, Feb. 2024, https://doi.org/10.1016/j.ijinfomgt.2023.102700

[12] P. Chatterjee, D. Das, and D. B. Rawat, "Federated Learning Empowered Recommendation Model for Financial Consumer Services," IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 2508–2516, Feb. 2024, https://doi.org/10.1109/TCE.2023.3339702

[13] S. Pingulkar and D. Pawade, "Federated Learning Architectures for Credit Risk Assessment: A Comparative Analysis of Vertical, Horizontal, and Transfer Learning Approaches," in 2024 IEEE International Conference on Blockchain and Distributed Systems Security, ICBDS 2024, Institute of Electrical and Electronics Engineers Inc., 2024. https://doi.org/10.1109/ICBDS61829.2024.10837430

[14] H. Abbassi, S. El Mendili, and Y. Gahi, "Adaptive, Privacy-Enhanced Real-Time Fraud Detection in Banking Networks Through Federated Learning and VAE-QLSTM Fusion," Big Data and Cognitive Computing, vol. 9, no. 7, Jul. 2025, https://doi.org/10.3390/bdcc9070185

[15] V. Venkata Krishna Reddy, R. Vijaya Kumar Reddy, M. Siva Krishna Munaga, B. Karnam, S. K. Maddila, and C. Sekhar Kolli, "Deep learning-based credit card fraud detection in federated learning," Expert Syst Appl, vol. 255, Dec. 2024, https://doi.org/10.1016/j.eswa.2024.124493

[16] Z. Wang, J. Xiao, L. Wang, and J. Yao, "A novel federated learning approach with knowledge transfer for credit scoring," Decis Support Syst, vol. 177, Feb. 2024, https://doi.org/10.1016/j.dss.2023.114084

[17] A. Oualid, Y. Maleh, and L. Moumoun, "FEDERATED LEARNING TECHNIQUES APPLIED TO CREDIT RISK MANAGEMENT: A SYSTEMATIC LITERATURE REVIEW," EDPACS, vol. 68, no. 1, pp. 42–56, 2023, https://doi.org/10.1080/07366981.2023.2241647

[18] A. A. Khan, A. Alsufyani, N. Alsufyani, and M. A. Mohamed, "BAML: a decentralized approach to secure, privacy-preserving financial compliance for enhancing anti-money laundering with blockchain hyperledger and federated learning," Peer Peer Netw Appl, vol. 18, no. 5, p. 270, 2025, https://doi.org/10.1007/s12083-025-02086-6

[19] S. K. Aljunaid, S. J. Almheiri, H. Dawood, and M. A. Khan, "Secure and Transparent Banking: Explainable AI-Driven Federated Learning Model for Financial Fraud Detection," Journal of Risk and Financial Management, vol. 18, no. 4, 2025, https://doi.org/10.3390/jrfm18040179

[20] Z. Zhao et al., "Federated Learning with Non-IID Data in Wireless Networks," IEEE Trans Wirel Commun, vol. 21, no. 3, pp. 1927–1942, Mar. 2022, https://doi.org/10.1109/TWC.2021.3108197

[21] Y. Fu, M. Dong, L. Zhou, C. Li, F. Richard Yu, and N. Cheng, "A Distributed Incentive Mechanism to Balance Demand and Communication Overhead for Multiple Federated Learning Tasks in IoV," IEEE Internet Things J, vol. 12, no. 8, pp. 10479–10492, 2025, https://doi.org/10.1109/JIOT.2024.3510561

[22] K. N. Kumar, C. K. Mohan, and L. R. Cenkeramaddi, "The Impact of Adversarial Attacks on Federated Learning: A Survey," IEEE Trans Pattern Anal Mach Intell, vol. 46, no. 5, pp. 2672–2691, May 2024, https://doi.org/10.1109/TPAMI.2023.3322785

[23] A. Zafar, "Quantum Computing in Finance: Regulatory Readiness, Legal Gaps, and the Future of Secure Tech Innovation," European Journal of Risk Regulation, pp. 1–32, 2025, https://doi.org/10.47852/bonviewaaes32021325

[24] C. C. Tan, T. G. Sharma, and V. Zhou, "Quantum Computing Threat Modelling on a Generic CPS Setup," 2021. [Online]. Available: http://go.qub.ac.uk/oa-feedback

[25] R. Thombre and B. Jajodia, "Experimental Analysis of Attacks on RSA & Rabin Cryptosystems using Quantum Shor's Algorithm," in Proceedings of International Conference on Women Researchers in Electronics and Computing, AIJR Publisher, Sep. 2021, pp. 587–596. https://doi.org/10.21467/proceedings.114.74

[26] H. H. Shadan and S. M. N. Islam, "Quantum Computing and Cybersecurity in Accounting and Finance in the Post-Quantum World: Challenges and Opportunities for Securing Accounting and Finance Systems," FinTech, vol. 4, no. 4, p. 52, Sep. 2025, https://doi.org/10.3390/fintech4040052

[27] A. Reddy, "Evaluating Post-Quantum Cryptography in the Era of Quantum Supremacy: Quantum Shadows," 2025.

[28] P. Das, "Quantum Computing in Payments Security: Preparing for the Post-Quantum Era."

[29] H. Y. Huang et al., "Power of data in quantum machine learning," Nat Commun, vol. 12, no. 1, Dec. 2021, https://doi.org/10.1038/s41467-021-22539-9

[30] A. Zeguendry, Z. Jarir, and M. Quafafou, "Quantum Machine Learning: A Review and Case Studies," Feb. 01, 2023, MDPI. https://doi.org/10.3390/e25020287

[31] Q. Le Wang et al., "An advanced quantum support vector machine for power quality disturbance detection and identification," EPJ Quantum Technol, vol. 11, no. 1, Dec. 2024, https://doi.org/10.1140/epjqt/s40507-024-00283-5

[32] N. K. Bhasin, S. Kadyan, K. Santosh, R. Hp, R. Changala, and B. K. Bala, "Enhancing Quantum Machine Learning Algorithms for Optimized Financial Portfolio Management," in 2024 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing, INCOS 2024 - Proceedings, Institute of Electrical and Electronics Engineers Inc., 2024. https://doi.org/10.1109/INCOS59338.2024.10527612

[33] C. Huot, K. Kea, T. K. Kim, and Y. Han, "Enhancing Knapsack-Based Financial Portfolio Optimization Using Quantum Approximate Optimization Algorithm," IEEE Access, vol. 12, pp. 183779–183791, 2024, https://doi.org/10.1109/ACCESS.2024.3506981

[34] Financial derivatives pricing using quantum neural networks- state-of-the-art".

[35] J. Zhou, "Quantum Finance: Exploring the Implications of Quantum Computing on Financial Models," Comput Econ, 2025, https://doi.org/10.1007/s10614-025-10894-4

[36] A. Boretti, "Technical, economic, and societal risks in the progress of artificial intelligence driven quantum technologies," Discover Artificial Intelligence, vol. 4, no. 1, Dec. 2024, https://doi.org/10.1007/s44163-024-00171-y

[37] "Modern finance through quantum computing-A systematic literature review".

[38] C. Qiao, M. Li, Y. Liu, and Z. Tian, "Transitioning From Federated Learning to Quantum Federated Learning in Internet of Things: A Comprehensive Survey," IEEE Communications Surveys and Tutorials, vol. 27, no. 1, pp. 509–545, 2025, https://doi.org/10.1109/COMST.2024.3399612

[39] T. Qayyum et al., "Quantum Federated Learning: Bridging Quantum Computing and Distributed AI," in Proceedings - 2024 IEEE/ACM 17th International Conference on Utility and Cloud Computing, UCC 2024, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 327–335. https://doi.org/10.1109/UCC63386.2024.00053

[40] A. Singh Bhatia and D. E. Bernal Neira, "Federated learning with tensor networks: a quantum AI framework for healthcare," Mach Learn Sci Technol, vol. 5, no. 4, Dec. 2024, https://doi.org/10.1088/2632-2153/ad8c11

[41] R. Kumar Inakoti, M. James Stephen, and P. Reddy, "ENHANCING QUANTUM CRYPTOGRAPHY WITH MACHINE AND DEEP LEARNING A HYBRID APPROACH FOR SECURE AND SCALABLE POST-QUANTUM SECURITY," J Theor Appl Inf Technol, vol. 15, no. 11, 2025, [Online]. Available: www.jatit.org

[42] M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," Mar. 29, 2021, BMJ Publishing Group. https://doi.org/10.1136/bmj.n71

[43] Y. Wang, Y. Gu, and X. Shen, "Anti-Collusion and Latency-Tolerant Privacy-Preserving Federated Learning Framework via Multi-Key Homomorphic Aggregation," in Proceedings - 2025 IEEE Conference on Artificial Intelligence, CAI 2025, Institute of Electrical and Electronics Engineers Inc., 2025, pp. 872–875. https://doi.org/10.1109/CAI64502.2025.00154

[44] N. Innan, A. Marchisio, M. Bennai, and M. Shafique, "QFNN-FFD: Quantum Federated Neural Network for Financial Fraud Detection," in Proceedings - 2025 IEEE International Conference on Quantum Software, QSW 2025, Institute of Electrical and Electronics Engineers Inc., 2025, pp. 41–47. https://doi.org/10.1109/QSW67625.2025.00015

[45] S. Darzi and A. A. Yavuz, "Counter Denial of Service for Next-Generation Networks within the Artificial Intelligence and Post-Quantum Era," in Proceedings - 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications, TPS-ISA 2024, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 138–147. https://doi.org/10.1109/TPS-ISA62245.2024.00025

[46] N. Innan, M. Kashif, A. Marchisio, M. Bennai, and M. Shafique, "Next-Generation Quantum Neural Networks: Enhancing Efficiency, Security, and Privacy," in Proceedings - 2025 IEEE 31st International Symposium on On-Line Testing and Robust System Design, IOLTS 2025, Institute of Electrical and Electronics Engineers Inc., 2025. https://doi.org/10.1109/IOLTS65288.2025.11116981

[47] R. Haripriya, N. Khare, M. Pandey, and S. Biswas, "Navigating the fusion of federated learning and big data: a systematic review for the AI landscape," Cluster Comput, vol. 28, no. 5, Oct. 2025, https://doi.org/10.1007/s10586-024-05070-6

[48] A. Garg, M. Singh, and M. Kumar, "The Intersection of Quantum Computing, Artificial Intelligence and Financial Risks: A Bibliometric Analysis of the Modern Financial Sector," Journal of Information Technology Management, vol. 17, pp. 3–23, 2025, https://doi.org/10.22059/JITM.2025.100694

[49] R. Baskerville and F. Rowe, "Integration of Information Systems and Cybersecurity Countermeasures: An Exposure to Risk Perspective."

[50] L. Leclerc et al., "Financial risk management on a neutral atom quantum processor," Phys Rev Res, vol. 5, no. 4, Oct. 2023, https://doi.org/10.1103/PhysRevResearch.5.043117

[51] S. Thakkar, S. Kazdaghli, N. Mathur, I. Kerenidis, A. J. Ferreira–Martins, and S. Brito, "Improved financial forecasting via quantum machine learning," Quantum Mach Intell, vol. 6, no. 1, Jun. 2024, https://doi.org/10.1007/s42484-024-00157-0.

[52] C. Ren et al., "Toward Quantum Federated Learning," 2025, Institute of Electrical and Electronics Engineers Inc.

https://doi.org/10.1109/TNNLS.2025.3552643

[53] A. S. Naik, E. Yeniaras, G. Hellstern, G. Prasad, and S. K. L. P. Vishwakarma, "From portfolio optimization to quantum blockchain and security: a systematic review of quantum computing in finance," Dec. 01, 2025, Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1186/s40854-025-00751-6

[54] A. Febryana Yuscatama Darmawan, "Zero-Trust Architecture Adaptation for Post-Quantum Cryptography: Implementation Roadmap for Critical Infrastructure," Journal of Economics, Technology and Business (JETBIS), vol. 4, 2025, [Online]. Available: https://jetbis.al-makkipublisher.com/index.php/al/index