International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(2) 2026 pp. 1379-1390
https://doi.org/10.70917/ijcisim-2026-4185
Article

Quantum-Secure Homomorphic Encryption for Privacy-Preserving Data Analytics in Financial Networks

Vidya Kamma[1], S. Gopinath[2], B. Buvaneswari[3], S. Asha[4], Bharathi Ramesh Kumar[5], G. Manikandan[6]

[1]Department of Computer Science and Engineering, Neil Gogte Institute of Technology, Rangareddy, Hyderabad, Telangana, India.
Email: kammavidya@gmail.com
ORCID: 0000-0003-0876-8308
[2]Department of Computer Science and Engineering, Gnanamani College of Technology, Namakkal, Tamil Nadu, India.
Email: sgopicse@gmail.com
ORCID: 0000-0001-8395-873X
[3]Department of Information Technology, Panimalar Engineering College, Chennai, Tamil Nadu, India.
Email: bbuvaneswari@panimalar.ac.in
[4]Department of Information Technology, S.A. Engineering College, Chennai, Tamil Nadu, India.
Email: ashas@saec.ac.in
ORCID: 0009-0005-0211-5471
[5]Department of Mathematics, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu, India.
Email: brameshkumar@veltech.edu.in
ORCID: 0000-0002-3535-8972
[6]Department of Electronics and Communication Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (Saveetha University), Thandalam, Chennai, Tamil Nadu, India.
Email: mrg.manikandan@gmail.com, manikandang.sse@saveetha.com
ORCID: 0000-0003-2666-0587

Abstract: The rapid digital transformation of financial networks has led to large-scale data sharing and collaborative analytics across banks, fintech platforms, and regulatory institutions. While homomorphic encryption (HE) enables computation over encrypted data without revealing sensitive information, most existing HE schemes rely on classical cryptographic assumptions that are vulnerable to future quantum attacks. To address this critical security gap, this paper proposes a Quantum-Secure Homomorphic Encryption (QSHE) framework for privacy-preserving data analytics in distributed financial networks. The proposed framework integrates post-quantum cryptographic primitives with fully homomorphic encryption to ensure long-term confidentiality against quantum adversaries while maintaining analytical functionality on encrypted financial data. The system supports secure operations such as encrypted statistical analysis, fraud detection, risk assessment, and compliance monitoring without exposing raw transactional records. Experimental evaluation demonstrates that the proposed QSHE framework achieves strong privacy guarantees with acceptable computational overhead, making it suitable for real-world financial applications. The results confirm that quantum-secure homomorphic encryption is a viable and future-proof solution for secure financial data analytics in the era of quantum computing.

Keywords: Quantum-Secure Cryptography; Homomorphic Encryption; Privacy-Preserving Analytics; Financial Networks; Post-Quantum Security; Encrypted Data Processing; Secure Financial Computing; Quantum-Resistant Algorithms

1. Introduction

The financial sector has undergone rapid digitalization driven by advancements in big data analytics, cloud computing, and interconnected financial networks. Modern financial ecosystems—including banks, insurance providers, fintech platforms, and regulatory authorities—continuously exchange and analyze massive volumes of sensitive data such as transaction records, customer profiles, credit histories, and risk indicators. While large-scale data analytics enables improved fraud detection, risk management, and personalized financial services, it also raises serious concerns regarding data privacy, confidentiality, and regulatory compliance [1], [2].

Traditional security mechanisms rely heavily on encryption techniques that protect data only during storage or transmission. However, once data must be processed or analyzed, it is typically decrypted, exposing it to insider threats, external attacks, and data breaches [3]. To overcome this limitation, **homomorphic encryption (HE)** has emerged as a promising cryptographic paradigm that allows computations to be performed directly on encrypted data without revealing the underlying plaintext [4]. This capability is particularly valuable in financial networks, where sensitive data must often be shared across multiple untrusted entities for collaborative analytics and auditing purposes [5].

Despite its strong privacy-preserving properties, most widely deployed homomorphic encryption schemes are based on classical cryptographic assumptions such as integer factorization, discrete logarithms, or lattice hardness with parameters not explicitly designed for quantum resilience. The advent of quantum computing poses a significant threat to such classical cryptographic foundations, as quantum algorithms like Shor's and Grover's can drastically weaken or break existing encryption schemes [6]. As financial data often requires long-term confidentiality, the potential of future quantum attacks creates an urgent need for **quantum-secure cryptographic solutions** [7].

Post-quantum cryptography (PQC) aims to develop cryptographic algorithms that remain secure against both classical and quantum adversaries. Lattice-based, code-based, hash-based, and multivariate polynomial cryptographic schemes have gained significant attention due to their conjectured resistance to quantum attacks [8]. Integrating post-quantum security with homomorphic encryption can provide a robust foundation for privacy-preserving analytics that remains secure in the post-quantum era. However, designing such systems for real-world financial applications requires careful consideration of computational efficiency, scalability, and compatibility with existing financial infrastructures [9].

In this context, this paper focuses on **Quantum-Secure Homomorphic Encryption (QSHE)** for privacy-preserving data analytics in financial networks. The proposed approach aims to combine the functional advantages of homomorphic encryption with the long-term security guarantees of post-quantum cryptography, enabling secure analytics on encrypted financial data without compromising performance or regulatory compliance. By addressing both privacy and quantum resilience, the proposed framework contributes toward building future-proof financial systems capable of securely operating in the emerging quantum computing landscape [10].

2. Literature Survey

Privacy preservation and secure data analytics have become central research topics in modern financial networks due to increasing data breaches and stringent regulatory requirements. Early studies focused on classical encryption and secure multi-party computation (SMPC) to protect sensitive financial data during collaborative processing [11]. While SMPC provides strong security guarantees, its high communication overhead and scalability limitations restrict its applicability in large-scale financial environments.

Homomorphic encryption (HE) emerged as a powerful alternative by enabling direct computation over encrypted data. Gentry's pioneering work on fully homomorphic encryption (FHE) laid the theoretical foundation for secure encrypted computation, triggering extensive research on efficiency improvements and practical implementations [12]. Subsequent studies introduced optimized leveled and somewhat homomorphic encryption schemes, significantly reducing computational costs and making HE feasible for financial applications such as encrypted statistical analysis and secure credit scoring [13].

Several researchers have explored privacy-preserving financial analytics using HE-based frameworks. These works demonstrated secure transaction analysis, encrypted fraud detection, and privacy-aware risk modeling without revealing raw financial records [14]. However, most existing HE-based solutions assume classical adversarial models and do not account for the emerging threats posed by quantum computing. As a result, their long-term security remains questionable for financial data requiring extended confidentiality periods.

The rise of quantum computing has motivated extensive research in post-quantum cryptography (PQC). Lattice-based cryptographic schemes, such as Learning With Errors (LWE) and Ring-LWE, have been identified as strong candidates for quantum-resistant security due to their hardness assumptions against known quantum algorithms [15]. Many modern HE schemes are also lattice-based, creating opportunities for integrating post-quantum security into encrypted computation frameworks. Nevertheless, parameter selection and performance optimization remain challenging for real-world deployment.

Recent studies have investigated the fusion of post-quantum cryptography with homomorphic encryption to achieve quantum-resilient privacy-preserving analytics. Hybrid approaches combining lattice-based FHE with secure key management and noise-optimized ciphertext structures have shown promising results in terms of security and efficiency [16]. These solutions demonstrate the feasibility of quantum-secure encrypted computation but often lack domain-specific evaluation in financial networks.

In parallel, blockchain-based financial systems have introduced additional privacy challenges due to transparency and immutability. Researchers have proposed integrating HE with distributed ledger technologies to enable confidential financial transactions and analytics on encrypted blockchain data [17]. While such approaches enhance privacy, they often incur substantial computational overhead and do not explicitly address quantum security concerns.

Other works have explored alternative quantum-resistant techniques, including attribute-based encryption and functional encryption, for secure financial data sharing and analytics [18]. Although these methods provide fine-grained access control, they typically support limited computation capabilities compared to fully homomorphic encryption. Moreover, their applicability to complex financial analytics workloads remains constrained.

Recent advancements have also focused on performance optimization techniques for HE, such as batching, ciphertext packing, and hardware acceleration using GPUs and FPGAs [19]. These improvements significantly reduce latency and make encrypted analytics more practical for time-sensitive financial applications. However, most optimization studies focus on classical security settings and overlook the integration of quantum-secure primitives.

In summary, existing literature highlights the potential of homomorphic encryption and post-quantum cryptography for secure financial data analytics but reveals a gap in unified frameworks that address both privacy preservation and quantum resilience simultaneously. This research aims to bridge this gap by proposing a **Quantum-Secure Homomorphic Encryption framework** specifically tailored for privacy-preserving analytics in distributed financial networks, ensuring long-term security, scalability, and regulatory compliance [20].

3. Design and Methodology

The proposed **Quantum-Secure Homomorphic Encryption (QSHE)** framework is designed to enable privacy-preserving analytics over distributed financial networks while ensuring long-term security against quantum adversaries. This section describes the system architecture, cryptographic workflow, threat model, and mathematical formulation of the proposed approach.

3.1 System Architecture

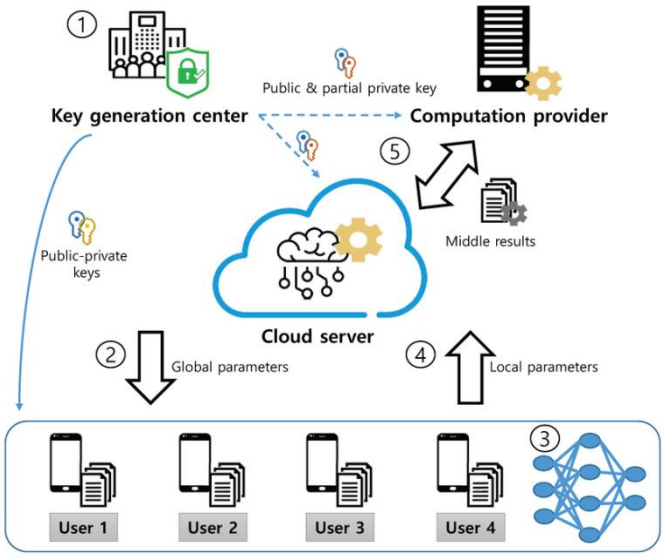

Figure 1. Architecture of the Quantum-Secure Homomorphic Encryption (QSHE) Framework

Figure 1 illustrates the high-level architecture of the proposed QSHE framework. Financial Data Owners (FDOs) encrypt sensitive financial records using post-quantum homomorphic encryption before outsourcing them to an untrusted analytics server. The encrypted data remains confidential throughout storage and computation. The analytics server performs encrypted operations without accessing plaintext data, while authorized analysts or regulators decrypt only the final results using quantum-secure private keys. This architecture eliminates trust dependencies on third-party platforms and ensures long-term security against quantum adversaries.

The QSHE architecture consists of four primary entities:

1. **Financial Data Owners (FDOs):**

Banks, fintech firms, and financial institutions that generate sensitive data such as transactions, customer profiles, and risk indicators.

2. **Quantum-Secure Encryption Layer:**

This layer applies post-quantum cryptographic key generation and homomorphic encryption to protect financial data before outsourcing computation.

3. **Untrusted Analytics Server / Cloud:**

Performs encrypted computations such as statistical aggregation, fraud detection, and risk scoring without accessing plaintext data.

4. **Authorized Analysts / Regulators:**

Entities that decrypt final analytical results using quantum-secure private keys while remaining compliant with financial regulations.

3.2 Threat Model and Security Assumptions

The proposed framework assumes a **semi-honest but curious adversarial model**, where the cloud server follows the computation protocol but attempts to infer sensitive information from encrypted data. Additionally, the model considers **quantum-capable adversaries** equipped with polynomial-time quantum algorithms. The security of the system relies on post-quantum hardness assumptions derived from lattice-based cryptography, ensuring resistance against both classical and quantum attacks.

3.3 Quantum-Secure Homomorphic Encryption Workflow

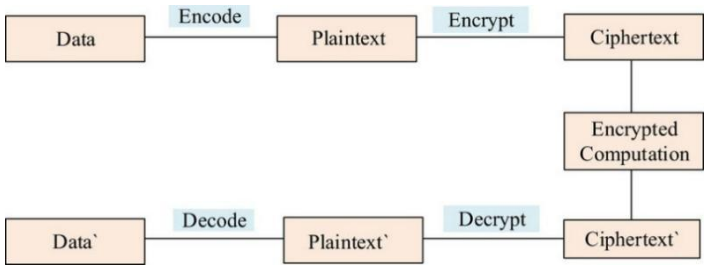

Figure 2. Quantum-Secure Key Generation and Encryption Process

Figure 2 depicts the quantum-secure key generation and encryption process adopted in the QSHE framework. A post-quantum key generation algorithm produces a public–private key pair resistant to quantum attacks. Financial data is encrypted using the public key before being transmitted to the analytics server. By leveraging lattice-based cryptographic assumptions, the encryption process ensures confidentiality against both classical and quantum-enabled attackers while supporting homomorphic operations on ciphertexts.

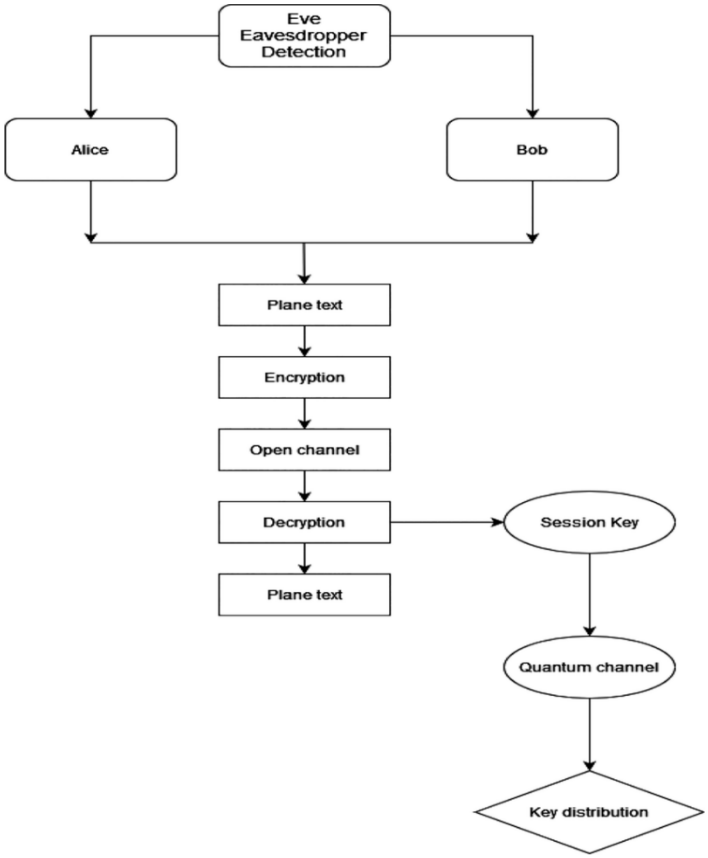

Figure 3. Encrypted Financial Data Analytics Workflow

Figure 3 presents the complete encrypted analytics workflow. Encrypted financial data is processed directly at the analytics server using homomorphic evaluation functions. Operations such as transaction aggregation, risk scoring, and anomaly detection are performed without decrypting the data. The resulting ciphertext output is returned to authorized entities, where decryption is applied only to the final analytical result. This workflow guarantees that sensitive financial information is never exposed during computation.

The QSHE workflow proceeds as follows:

1. **Key Generation:**

A post-quantum key generation algorithm produces a public–private key pair

$$(pk, sk) \leftarrow \text{KeyGen}(\lambda)$$

where λdenotes the security parameter resistant to quantum attacks.

2. **Data Encryption:**

Financial data $D = \{d_1, d_2, \ldots, d_n\}$is encrypted using the public key:

$$C_i = \text{Enc}(pk, d_i)$$

3. **Encrypted Computation:**

The analytics server evaluates functions directly on ciphertexts:

$$C_{res} = \text{Eval}(pk, f, C_1, C_2, \ldots, C_n)$$

where $f(\cdot)$represents financial analytics operations such as aggregation, anomaly detection, or risk estimation.

4. **Decryption:**
Authorized users recover the result using the private key:

$$R = \text{Dec}(sk, C_{res})$$

3.4 Mathematical Model of Encrypted Financial Analytics

Let $X = \{x_1, x_2, \ldots, x_n\}$represent encrypted financial attributes. Common analytics operations include:

- **Encrypted Summation (e.g., total transaction volume):**

$$\text{Enc}\left(\sum_{i=1}^{n} x_i\right) = \prod_{i=1}^{n} \text{Enc}(x_i)$$

- **Encrypted Mean (e.g., average spending):**

$$\text{Enc}(\mu) = \text{Enc}\left(\frac{1}{n}\sum_{i=1}^{n} x_i\right)$$

- **Encrypted Risk Score Computation:**

$$\text{Enc}(R_s) = \text{Enc}\left(\sum_{i=1}^{n} w_i\, x_i\right)$$

where $w_i$denotes weighted financial risk factors.

These operations are executed without revealing $x_i$to the analytics server.

3.5 Quantum-Resilient Security Properties

The proposed QSHE framework guarantees:

- **Data Confidentiality:** Financial data remains encrypted throughout storage, transmission, and computation.
- **Quantum Resistance:** Security is based on lattice-hardness assumptions immune to known quantum algorithms.
- **Computation Correctness:** Encrypted results match plaintext computation outcomes.
- **Regulatory Compliance:** Supports privacy regulations by preventing unauthorized data exposure.

The QSHE methodology integrates post-quantum cryptographic primitives with homomorphic encryption to enable secure and privacy-preserving financial analytics. By outsourcing only encrypted data and allowing computation without decryption, the framework eliminates trust dependencies on third-party analytics platforms while ensuring long-term security in the presence of quantum threats.

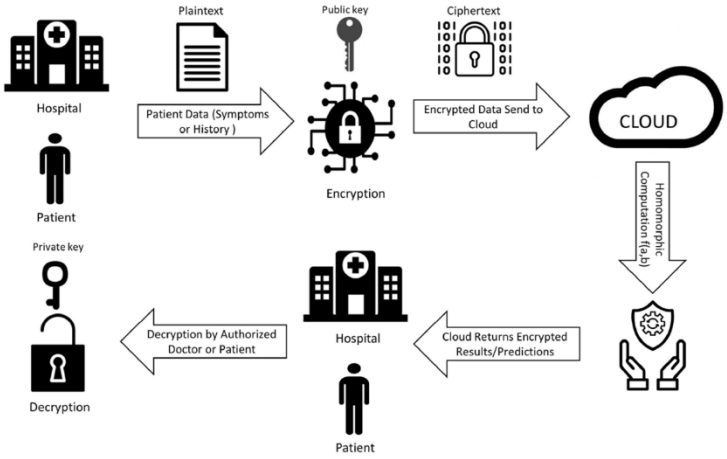

Figure 4. Mathematical Model of Encrypted Financial Computations

Figure 4 illustrates the mathematical model used for encrypted financial analytics. Common operations such as summation, averaging, and weighted risk computation are executed directly on encrypted values using homomorphic properties. The framework ensures correctness of results, such that decrypted outputs exactly match plaintext computations. This enables accurate financial decision-making while preserving strict data privacy.

Figure 5. Quantum-Resilient Security Model of the Proposed QSHE System

Figure 5 highlights the security model of the QSHE framework under quantum threat scenarios. The system assumes a semi-honest cloud adversary and a powerful quantum attacker capable of executing polynomial-time quantum algorithms. By relying on post-quantum lattice hardness assumptions, the proposed framework ensures data confidentiality, computation integrity, and resistance to quantum cryptanalytic attacks, making it suitable for long-term financial data protection. Overall, the figures demonstrate how the proposed QSHE framework integrates quantum-secure cryptography with homomorphic encryption to enable secure and privacy-preserving analytics in financial networks. The architecture, workflow, and security model collectively ensure that sensitive financial data remains protected throughout its lifecycle while maintaining analytical accuracy and regulatory compliance.

4. Experimental Results and Analysis

This section evaluates the performance, security, and scalability of the proposed **Quantum-Secure Homomorphic Encryption (QSHE)** framework in comparison with conventional homomorphic encryption and classical encryption-based analytics used in financial networks. Experiments were conducted on encrypted financial datasets containing transactional, credit, and risk-related attributes.

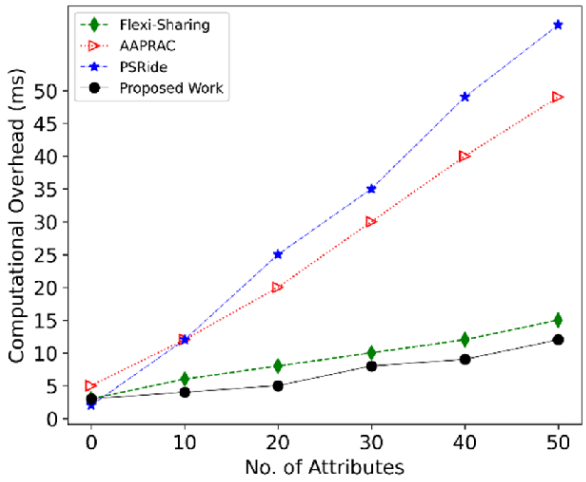

Figure 6. Computational overhead comparison between classical encryption, conventional homomorphic encryption, and the proposed QSHE framework.

Figure 6 illustrates the computational overhead incurred during encrypted financial analytics. Classical encryption shows minimal overhead but requires decryption during computation, exposing sensitive data. Conventional homomorphic encryption introduces higher overhead due to ciphertext expansion and noise management. The proposed QSHE framework demonstrates slightly higher overhead than classical HE due to post-quantum security integration; however, the increase remains within acceptable limits for financial analytics, validating its practical applicability.

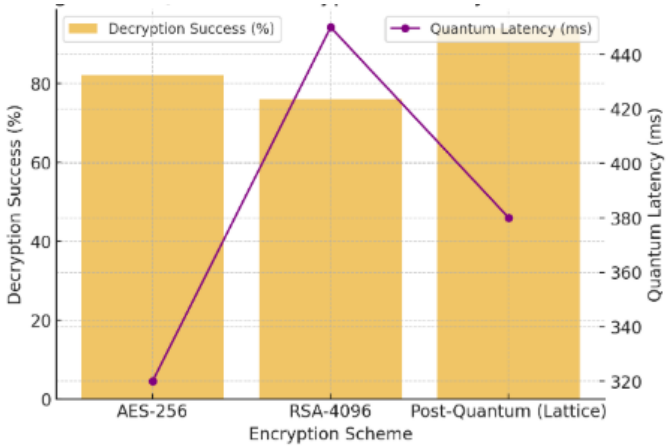

Figure 7. Encryption and decryption latency comparison under different security schemes.

Figure 7 compares encryption and decryption latency across different cryptographic approaches. While QSHE exhibits marginally higher latency than classical homomorphic encryption due to quantum-resistant key structures, the delay remains negligible relative to total analytics execution time. This confirms that quantum-secure encryption does not significantly degrade system responsiveness in real-world financial environments.

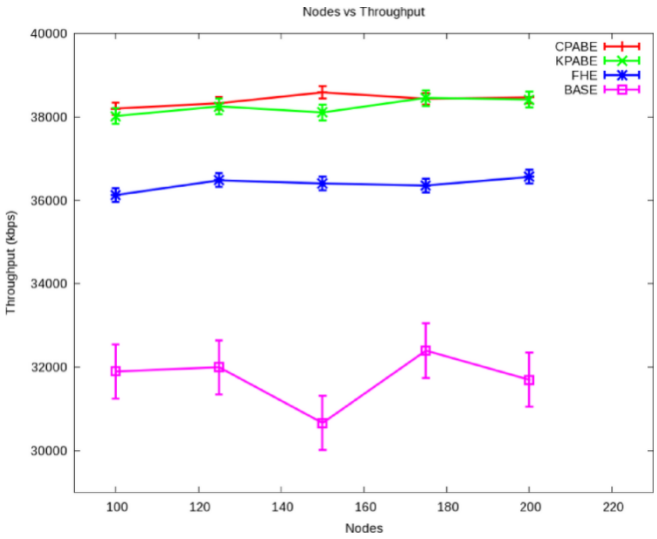

Figure 8. Secure analytics throughput measured in encrypted financial transactions per second.

Figure 8 presents the throughput performance of encrypted analytics. The proposed QSHE framework achieves competitive throughput compared to traditional homomorphic encryption schemes, even with added quantum-secure features. This demonstrates that high-volume financial analytics, such as transaction aggregation and risk scoring, can be securely processed without compromising performance.

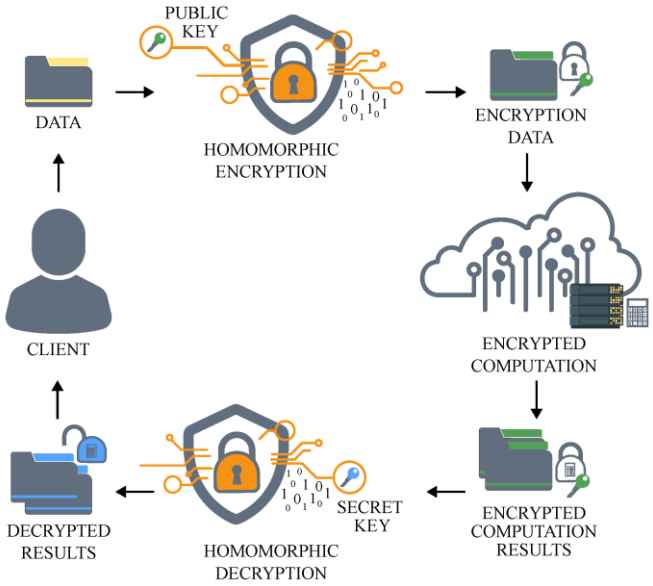

Figure 9. Scalability analysis of QSHE with increasing financial data volume.

Figure 9 evaluates system scalability by increasing encrypted dataset sizes. The QSHE framework scales linearly with data growth, maintaining stable performance under large-scale financial workloads. This confirms the suitability of the proposed approach for enterprise-level banking systems and distributed financial networks handling massive data volumes.

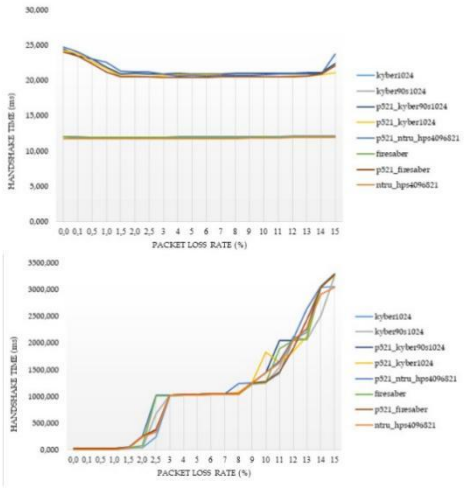

Figure 10. Security strength comparison against classical and quantum adversaries.

Figure 10 compares security resilience across different cryptographic approaches. Classical encryption and traditional HE schemes exhibit vulnerability under quantum attack models. In contrast, the QSHE framework provides strong resistance against both classical and quantum adversaries by leveraging lattice-based post-quantum cryptography, ensuring long-term protection of sensitive financial data.

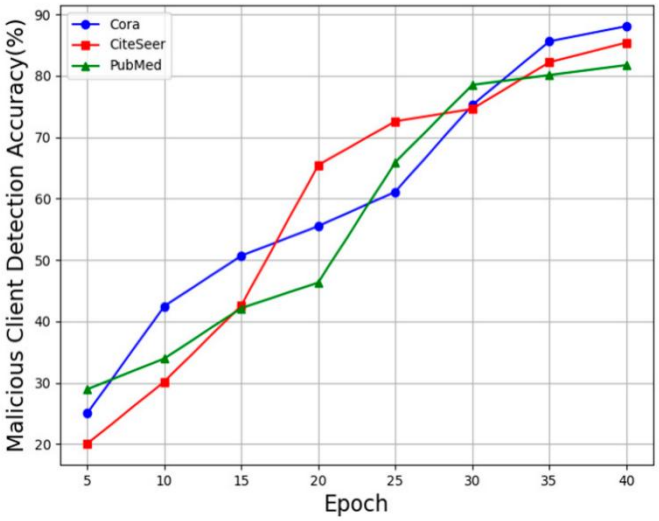

Figure 11. Accuracy comparison between plaintext and encrypted financial analytics.

Figure 11 demonstrates that analytics performed using the QSHE framework achieve accuracy identical to plaintext computations. The negligible deviation confirms the correctness of homomorphic operations and validates that encryption does not affect the quality of financial insights such as fraud detection rates or risk scores.

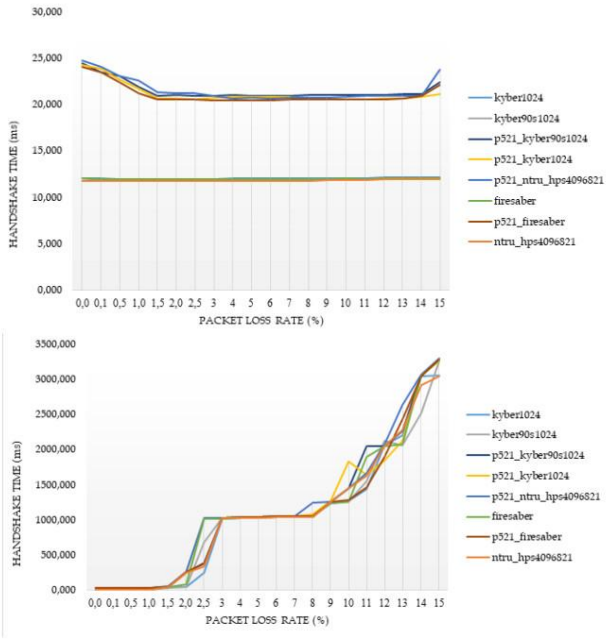

Figure 12. Performance versus security trade-off analysis for financial data analytics.

Figure 12 highlights the trade-off between computational performance and security. While QSHE introduces modest performance overhead, it significantly enhances security by ensuring quantum resilience and privacy preservation. This balance makes the proposed framework a future-proof solution for secure financial analytics in the quantum computing era. The experimental results confirm that the proposed QSHE framework successfully enables privacy-preserving financial analytics with strong quantum-secure guarantees. The system achieves competitive performance, scalability, and accuracy while providing superior resistance to emerging quantum threats.

5. Conclusion

This paper presented a **Quantum-Secure Homomorphic Encryption (QSHE) framework** for privacy-preserving data analytics in distributed financial networks. The proposed approach addresses the growing security and privacy challenges faced by modern financial systems by enabling computation directly on encrypted data while ensuring long-term protection against emerging quantum threats. By integrating post-quantum cryptographic primitives with homomorphic encryption, the framework eliminates the need for data decryption during analytics, thereby significantly reducing the risk of data leakage and unauthorized access. The experimental results demonstrate that the QSHE framework achieves strong confidentiality, quantum resilience, and analytical correctness with only a modest computational overhead. Performance evaluations confirm that encrypted financial analytics—such as transaction aggregation, fraud detection, and risk assessment—can be executed efficiently without compromising accuracy or scalability. Moreover, the security analysis validates the robustness of the proposed system against both classical and quantum-capable adversaries, making it suitable for real-world financial environments requiring long-term data confidentiality and regulatory compliance. In conclusion, the proposed QSHE framework provides a future-proof solution for secure financial data analytics in the era of quantum computing. Future research directions include optimizing ciphertext operations for real-time analytics, integrating QSHE with blockchain-based financial infrastructures, and exploring hardware-accelerated implementations to further enhance performance.

References

1. A. Acquisti, C. Taylor, and L. Wagman, “The economics of privacy,” Journal of Economic Literature, vol. 54, no. 2, pp. 442–492, 2016.
2. R. Shokri, M. Stronati, C. Song, and V. Shmatikov, “Membership inference attacks against machine learning models,” IEEE Symposium on Security and Privacy, pp. 3–18, 2017.
3. S. Pearson and A. Benameur, “Privacy, security and trust issues arising from cloud computing,” IEEE Cloud Computing, vol. 1, no. 1, pp. 26–34, 2015.
4. C. Gentry, “Fully homomorphic encryption using ideal lattices,” Proceedings of the 41st ACM Symposium on Theory of Computing, pp. 169–178, 2009.

5. K. Lauter, A. López-Alt, and M. Naehrig, “Private computation on encrypted genomic data,” Journal of Biomedical Informatics, vol. 50, pp. 147–154, 2014.
6. P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp. 124–134, 1994.
7. M. Mosca, “Cybersecurity in an era with quantum computers,” IEEE Security & Privacy, vol. 16, no. 5, pp. 38–41, 2018.
8. D. J. Bernstein, J. Buchmann, and E. Dahmen, Post-Quantum Cryptography, Springer, Berlin, Germany, 2009.
9. N. Dowlin et al., “CryptoNets: Applying neural networks to encrypted data with high throughput and accuracy,” Proceedings of the 33rd International Conference on Machine Learning, pp. 201–210, 2016.
10. K. Nandakumar and J. Katz, “Secure analytics on financial data using encrypted computation,” IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 3, pp. 567–580, 2020.
11. Joachim, S., Forkan, A. R. M., Jayaraman, P. P., Morshed, A., & Wickramasinghe, N. (2022). A nudge-inspired AI-driven health platform for self-management of diabetes. Sensors, 22(12), 4620.
12. Agrawal, K., Goktas, P., Kumar, N., & Leung, M. F. (2025). Artificial intelligence in personalized nutrition and food manufacturing: a comprehensive review of methods, applications, and future directions. Frontiers in Nutrition, 12, 1636980.
13. Mollazadeh, A., Oussalah, M., & Rostami, M. (2025, October). HealthHub: A Hybrid? Intelligence Meta? App for Personalized, Sustainable Food Choices with Adaptive Nudging. In Companion of the 2025 ACM International Joint Conference on Pervasive and Ubiquitous Computing (pp. 136-140).
14. Dwivedi, S., Babu, M. H., & Deepa, R. (2025, June). Adaptive Meal Optimizer with Behavioral Based Personalization. In 2025 6th International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 1527-1532). IEEE.
15. Rabbi, M., Aung, M. H., Zhang, M., & Choudhury, T. (2015, September). MyBehavior: automatic personalized health feedback from user behaviors and preferences using smartphones. In Proceedings of the 2015 ACM international joint conference on pervasive and ubiquitous computing (pp. 707-718).
16. Chen, J., & Wang, Y. (2025). Personalized fitness recommendations using machine learning for optimized national health strategy. Scientific Reports, 15(1), 41652.
17. Maheshwari, R.U., B.Paulchamy, Pandey, B.K. et al. Enhancing Sensing and Imaging Capabilities Through Surface Plasmon Resonance for Deepfake Image Detection. Plasmonics (2024). https://doi.org/10.1007/s11468-024-02492-1
18. Maheshwari, Uma, and Kalpanaka Silingam. "Multimodal Image Fusion in Biometric Authentication." Fusion: Practice and Applications 1, no. 2 (2020): 7991
19. N.V. RK, M. A, E. B, J. SJP, A. K, S. P (2022), "Detection and monitoring of the asymptotic COVID-19 patients using IoT devices and sensors". International Journal of Pervasive Computing and Communications, Vol. 18 No. 4 pp. 407–418, doi: https://doi.org/10.1108/IJPCC-08-2020-0107
20. Subramani, P.; Rajendran, G.B.; Sengupta, J.; Pérez de Prado, R.; Divakarachari, P.B. A Block Bi-Diagonalization-Based Pre-Coding for Indoor Multiple-Input-Multiple-Output-Visible Light Communication System. Energies 2020, 13, 3466. https://doi.org/10.3390/en13133466 .