THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 5. Issue 3 (2025)
https://doi.org/10.62019/abbdm.v5i3.365

Post-Quantum Cryptography for Big Data Security

Muhammad Talha Tahir Bajwa, Muhammad Nabeel Afzal, Muhammad Hamza Afzal, Muhammad Sana Ullah*, Talha Umar, Haris Maqsood,

Chronicle

Article history
Received: June 04, 2025
Received in the revised format: June 18, 2025
Accepted: July 27, 2025
Available online: Aug 19, 2025

Muhammad Talha Tahir Bajwa, Muhammad Nabeel Afzal & Muhammad Sana Ullah are currently affiliated with the Department of Computer Science University of Agriculture Faisalabad, Pakistan.
Email: talhabajwa6p@gmail.com
Email: nabeelafzal361@gmail.com
Email: msanaullah133@gmail.com

Muhammad Hamza Afzal is currently affiliated with the Department of Computer Science, MNS University of Engineering and Technology, Multan, Pakistan.
Email: hamzaafzal67112@gmail.com

Talha Umar is currently affiliated with the Department of Computer Science, Comsats University Islamabad, Pakistan.
Email: talhaumar4373@gmail.com

Haris Maqsood is currently affiliated with the School of Department of Software Engineering, Lahore Garrison University, Pakistan.
Email: harismaqsood58@gmail.com

Corresponding Author*

Abstract

The emergence of quantum computing is a severe threat to traditional encryption technologies particularly those applied to large-scale data environments. Since big data systems are based on encryption algorithms that can theoretically be broken using quantum algorithms such as Grovers and Shors, big data systems are especially susceptible. Big data systems are characterized by huge volume, velocity and variety. Post-Quantum Cryptography (PQC) offers a proactive way of safeguarding such systems through the use of quantum-resistant algorithms that include hash-, lattice-, code-, and multivariate polynomial algorithms. This work discusses how PQC can be incorporated into big data infrastructures, particularly in distributed environments such as Hadoop and Spark, secure storage and real-time processing. Potential solutions are discussed along with such crucial topics as interoperability, computing overhead, and classical-to-quantum-safe standard transition. By adopting an early form of implementation of PQC, organizations can future-proof their big data security framework against an evolving quantum threat landscape.

Keywords: Post-Quantum Cryptography, Big Data Security, Quantum Computing Threats, Quantum-Safe Encryption, Spark Security, Cryptographic Migration.

INTRODUCTION

Due to the emergence of quantum computing, which promises quite a paradigm shift in the cryptography field, many classical cryptographic techniques such as RSA, ECC, Diffie-hellman and DSA will find themselves threatened by new attack vectors, unheard of by now. The most significant of those is the method of Shor which, theoretically, can allow to factor big integers and compute discrete logarithms in efficient ways, thus compromising the safety of widely used public-key systems [1]. This poses a serious threat to the confidentiality and integrity of the data over digital infrastructures. These quantum threats are even more dangerous to Big Data ecosystems that are characterized by the three Vs, a possession of volume, velocity, and variety [4]. These ecosystems deal with sensitive data sets that require security into the long term and often have to use distributed systems such as Hadoop and Spark. There is also the possibility of "harvest now, decrypt later" scenario where

adversaries can capture data that currently uses encrypted data and in the future wait until quantum capabilities become more feasible and decrypt the data [2]. Post-Quantum Cryptography (PQC) offers this defence by applying quantum resistant algorithms that are based on complex mathematical constructions and are less resistant to quantum attacks [5]. All these schemes have varying trade-offs in performance, key sizes and complexity of implementation. These are lattice-based schemes (such as CRYSTALS-Kyber and CRYSTALS-Dilithium), code-based schemes, hash-based schemes, multivariate polynomial schemes and isogeny-based schemes [6]. Assessment and support of such algorithms have been fundamental in the NIST PQC standardization effort.

Three of these algorithms, namely, FIPS 203 (ML-KEM/Kyber), FIPS 204 (ML-DSA/Dilithium), and FIPS 205 (SLH-DSA/SPHINCS+) were officially approved as of August 2024. HQC, an algorithmic technique, was selected as a backup in March 2025 and full standardisation is now underway [3]. The world is sensitized on the need of migration urgency. For example, in order to prevent hurried implementations and security failings, the National Cyber Security Centre (NCSC) of the United Kingdom has advised enterprises to start planning by 2028 and strive for full deployment by 2035. The migration of federal systems is also expected to start between 2025 and 2030, according to NIST's roadmap. Despite this advice, industries are still ill-prepared. Nearly half of firms in North America and Europe, particularly mid-sized ones, are not yet prepared to handle cybersecurity challenges of the quantum age, according to a new poll. The need for focused frameworks and governmental assistance is further shown by the fact that readiness scores in India's banking and financial sector averaged only 2.4 out of 5.

Making the switch to PQC in Big Data systems presents a number of complex difficulties. Especially for real-time data processing pipelines, the computational overhead, which includes increased key and signature sizes, might strain storage and bandwidth and impair system performance. Hybrid or dual-stack techniques are required for interoperability with legacy protocols and platforms (such as TLS, HDFS, and PKI) [7]. Asset inventory, risk assessment, phased adoption, vendor engagement, crypto-agility, hybrid deployments, testing, staff training, and final decommissioning of outdated systems are all common steps in a systematic transition roadmap. Also, the ability to replace algorithms will be key to the future resilience cryptographic agility. Migration can be offered through hybrid PQCclassical approaches because the compatibility of the methods is offered as part of the transition process. To address the issue of the evolving standards and implementation challenges every organization needs to invest in skills development and revise the security policies on a frequent.

Figure 1.
PQC Integration for Big Data Security against Quantum Threats

Overview of Cryptography in the Quantum Era

Cryptography has been at the center of data security since it ensures confidentiality, integrity and authenticity of communication in the realm of digital communication. Classical cryptography systems such as RSA, DiffieHellman (DH) and elliptic Curve Cryptography (ECC) relate to the computational complexity of mathematical problems such as integer factorization and discrete logarithms. These schemes have shown the robustness to traditional computers, enabling secure data transfer across big data ecosystems, e.g., cloud platforms, distributed storage systems and large-scale analytics frameworks. With such an introduction of quantum computer, however, the security situation changes radically. Owing to their capacities to effectively decipher security presumptions, quantum algorithms, particularly Shor algorithm, are a menace to the generally deployed asymmetric cryptographic primitives [20].

Likewise, reduction of the complexity of brute-force searches under Grover makes symmetric-key systems vulnerable as they need bigger keys to achieve the same security level. [18]. These developments put enormous stores of private Big Data, from medical databases to banking records, at risk of being decrypted when scalable quantum computers become available. Therefore, Big Data settings face two challenges in the quantum era. On the one hand, attackers might use "harvest now, decrypt later" tactics, gathering encrypted datasets now in anticipation of decryption made possible by quantum technology in the future. However, the potential impact of cryptographic flaws is increased by the dynamic and dispersed nature of Big Data infrastructure, which includes Hadoop clusters, Spark engines, NoSQL databases, and multi-cloud storage. Long before quantum computers are mature, these vulnerabilities must be anticipated in order to ensure long-term data security [22].

Post-Quantum Cryptography (PQC) has become a promising remedy to this impending danger. In contrast to QKD, which is dependent on specialized hardware, PQC uses mathematical problems that are thought to be impervious to both classical and quantum attacks. The U.S. National Institute of Standards and Technology (NIST) is now working hard to standardize families of PQC algorithms, such as lattice-based, code-based, multivariate, and hash-based methods [19]. Quantum-resistance PQC in Big Data systems will ensure that the Big Data systems are also resilient to developed threats during the quantum era besides being compatible to the future cryptographic standards [17]. Thus, the post-quantum context will shift cryptography beyond the conventional methods of security assumptions to the intersectional paradigm that presupposes the incorporation of quantum-safe processes into the Big Data security infrastructure. This shift highlights the urgency of overcoming the implementation of PQC to mitigate the large datasets at any point in their lifecycle, including processing and storage and transmission, to ensure the protection and integrity of crucial estimations in a post-quantum world.

Classical Computing vs Quantum Computing

The significant superiority of quantum computers to classical for completing certain tasks is known as quantum speedup. Entanglement and superposition are quantum processes conferring this advantage. Thanks to superposition, qubits can be in many states at once, and through the use of entanglement, qubits can be linked so that they exponentially increase the processing capacity of certain calculations. The most noticeable inefficiencies where this quantum speedup when using quantum computers can occur are tasks involving large amounts of data to process or complex

optimization problems to solve. Since it provides a physical perspective of the operational advantage of quantum computing, entanglement is significant in achieving quantum speedup especially in scalating the limitation of classical information computing. Quantum speedup is applicable to data processing at scale, complex simulations, optimization in problem solving, and other applications. As an example, the quantum algorithms are expected to significantly reduce the number of time required in the simulations involved in areas like medicine development, climate or even in materials science. Some of these skills are also applicable to solve complex optimization which arise in network architecture, finance, and logistics. Quantum computers are apt to error because quantum states are delicate. Decoherence is the phenomenon through which the quantum characteristics are lost by quantum bits (qubits) because of their interaction with surrounding environment. Quantum error correction forms a severe research field in quantum computation due to this susceptibility.

Quantum error correction uses sophisticated low-level techniques to detect and correct mistakes by using extra qubits. These techniques do not cause the quantum state to collapse since the quantum information is not actually measured. Instead, they can detect and correct errors without degrading, or damaging, the authenticity of the quantum computation. It is required to take reliable quantum computation, but with additional complexity of algorithms and increased number of qubits, boosting the resources demands of quantum computers. There is a need to introduce new strategies to avoid the impact of these negative effects; however, the approach can equally generate inaccurate and misleading data. On certain tasks, quantum computers can be less energy-intensive than classical computers. This expediency is based on the fact that quantum computers have innate potential to perform certain calculations than the number of operations that can be performed on conventional computers. This entails that the quantum computers have the potential to do everything that the conventional computers do but in a much smaller amount of energy on those things that are better done by the latter.

The energy efficiency of quantum computers has an especially important effect in areas where large scale simulations are vital. As an example, quantum computers may better simulate atomic and molecular interactions to study material science, which enables faster and even low-energy breakthroughs. As is the case, quantum computers have the potential to accelerate drug discovery processes within the pharma industry by enhancing the simulation tasks of complex molecular behavior which would require prohibitively large processing resources within a classical computer.

Implications for Cryptography

Quantum computers based on algorithms such as Shor severely threaten current cryptographic algorithms, in particular, public-key cryptography. Such algorithms employ quantum mechanics to solve discrete logarithm and integer factorization problems central to many other encryption methods in common use, such as RSA and the ECC. A major fraction of the current encryption methods is vulnerable to quantum computers since they can solve such problems very efficiently. This weakness poses major doubts on the security of data since it may allow quantum computers to decipher encrypted personal information encrypted with current methods. Two of the most widely-used cryptographic system, RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), are based on the elliptic curve discrete logarithm problem and the difficulty of integer factorization respectively. These cryptographic

schemes fail in an age of quantum computing because quantum computing, specifically Shor algorithm can crack such problems at a much faster rate than modern computers. This has brought about a lot of exploration on the exact quantum resources required to destroy such systems and at what time such an evolution could take place.

Development of Post-Quantum Cryptography

As a reaction to the quantum threat, the area of post-quantum cryptography focuses on the invention of cryptographic algorithms that should be resistant to conventional and quantum computing attacks. Other issues in mathematics that are believed to be unbreakable by quantum computer are under research in this field. Some of these issues include explosive lattice-based problems, multivariate polynomials, and hash-based cryptography. These have advantages and disadvantages to them, and tests are being undergone to determine their feasibility and efficiency.

Research and Innovation in Post-Quantum Cryptography

The research in this area also targets learning the security implications, efficiency, and implementation issues of new algorithms along with creating them, so it is post-quantum cryptography research. As an illustration, the speed of the key generation and encryption process and its perceived ability to resist quantum attacks provide the foundation to consider lattice-based cryptographic systems to be promising. Scientists are making efforts to defeat problems such as the complexity of implementation in existing infrastructures and the growth of key size.

Global Efforts and Standardization

Cryptography communities and international organizations are now trying to establish the international standards of post quantum cryptography with growing realization of the mass impact of quantum computing on encryption schemes. Institutions like the National Institute of Standards and Technology (NIST) in the United States are leading in implementing the evaluation and standardization of the algorithms of the post-quantum cryptography. In the bid to ensure the security, efficiency and compatibility of these new cryptographic systems in a variety of applications, such initiatives involve a rigorous verification and evaluation.

Along with being a technical issue, transitioning to post-quantum cryptography means a policy and regulatory issue, too. To keep the communication and data safe, the governments and businesses should cope with adoption problems of new cryptographic standards. This is in the form of adapting security processes, requirements on compliance and legal frameworks to emerging cryptographic technologies.

Layered Security Structure for PQC

Figure 1 displays the layered security architecture of PQC in the Big Data Security, in which a variety of components are combined in Big Data Security to help guard large-scale data systems against emerging quantum attacks.

Quantum Threats

The term "quantum threats" describes the security threats brought forth by the enormous processing capability of quantum computers. Commonly used classical cryptographic techniques like RSA, elliptic-curve cryptography (ECC), and Diffie-

Hellman (DH) can be cracked much more quickly with algorithms like Shor's and Grover's. This implies that once quantum computers are powerful enough, encrypted datasets that are now thought to be secure may become vulnerable in the setting of large data. Data confidentiality over the long run is seriously threatened by the possibility of retroactive decryption [8].

Harvest Now, Decrypt Later

The Harvest Now, Decrypt Later threat paradigm is closely related to this, wherein attackers store encrypted material now with the goal of decrypting it later when quantum-capable systems become available. Sensitive information having a lengthy "security shelf life," such government communications, corporate secrets, and medical records, is particularly at risk from this. This method exposes data to future exposure even in the absence of an immediate quantum attack [9].

Big Data Ecosystem

The Big Data Ecosystem, which stands for the frameworks, tools, and infrastructure needed to store, process, and analyze large and varied datasets, is at the core of the framework. High-performance processing engines like Apache Spark (whale image) and massive distributed systems like Apache Hadoop (elephant icon) are examples of this. Relational and NoSQL databases are indicated by database icons, and scalable big data processing and storage are made possible by cloud platforms such as AWS, Azure, and Google Cloud. Because these systems manage massive amounts of sensitive data, it is essential to implement robust encryption and cutting-edge security measures.

PQC Solutions

PQC Solutions, which are cryptographic algorithms made to withstand both conventional and quantum attacks, are found all across the ecosystem. These include code-based cryptography (e.g., Classic McEliece, HQC), which is based on decades of proven security; hash-based schemes (e.g., SPHINCS+), which rely on the strength of cryptographic hash functions; multivariate systems (e.g., Rainbow, GeMSS), which rely on solving multivariate polynomial equations over finite fields; and lattice-based techniques (e.g., CRYSTALS-Kyber, Dilithium), which are currently leading in NIST's PQC standards. In order to preserve secrecy, integrity, and authenticity in the quantum era, these techniques work together to create a protective "shield" surrounding the big data environment.

Big Data Security

Last but not least, the Big Data Security layer, represented by the lock icon at the diagram's base, stands for the ultimate goal: protecting the data lifecycle from processing to transmission to storage [10]. This involves the process of managing cryptographic keys with PQC-enabled systems, having strict access control and authentication mechanisms, encrypting data in transit and data at rest, and ensuring that compliance regulations such as GDPR and HIPAA are upheld. Even though PQC provides the basic protection against the decryption of quantum, these other security measures are required to provide full protection in order to manage a large scope of threats [11].

Table 1.
Diagram Elements and Their Roles in PQC for Big Data Security

Diagram Element	Meaning	Example Technologies / Concepts	Role in PQC for Big Data Security
Quantum Threats	Risks from quantum computers capable of breaking classical encryption.	Shor's algorithm, Grover's algorithm	Drives the need for replacing vulnerable encryption methods with quantum-resistant algorithms.
Harvest Now, Decrypt Later	Attack model where encrypted data is stolen today and decrypted in the future when quantum resources are available.	Nation-state data harvesting, data espionage	Highlights urgency to secure data now to protect long-term confidentiality.
Big Data Ecosystem	Platforms, tools, and infrastructure for large-scale data storage, processing, and analytics.	Apache Hadoop, Apache Spark, NoSQL DBs, cloud platforms (AWS, Azure, GCP)	PQC must integrate seamlessly into these systems without disrupting performance.
Lattice-Based Cryptography	PQC category based on hard lattice problems resistant to quantum attacks.	CRYSTALS-Kyber, CRYSTALS-Dilithium	Provides strong encryption and digital signatures with relatively efficient performance for big data workloads.
Code-Based Cryptography	PQC category relying on decoding error-correcting codes.	Classic McEliece, HQC	Offers proven security history, suitable for securing stored and transmitted data.
Hash-Based Cryptography	PQC category using hash functions for signatures.	SPHINCS+	Provides stateless and stateful signature schemes for secure data integrity in distributed systems.
Multivariate Cryptography	PQC category using systems of multivariate polynomial equations over finite fields.	Rainbow, GeMSS	Useful for digital signatures in high-throughput big data pipelines.
PQC Shield (Outer Layer)	Visual representation of PQC protecting big data systems from quantum threats.	NIST PQC standards	Serves as the core defense mechanism in a quantum-safe architecture.
Big Data Security (Lock Icon)	Ensuring confidentiality, integrity, and availability of data.	PQC-enabled TLS, PQC key management, access controls	Represents the ultimate goal — safeguarding sensitive big data against both classical and quantum attacks.

LITERATURE REVIEW

The experimental framework proposed in a recent study [15] allows comparing the aspects of several algorithms of post-quantum cryptography (PQC): hash-based (SPHINCS+), code-based (McEliece), and lattice-based (Kyber, Dilithium) in the context of high-performance cloud systems and resource-limited devices. The findings are that although code-based and hash-based systems can often be susceptible to larger key sizes and slower running in constrained environments, lattice-based algorithms, such as Kyber, offer a positive balance between security and speed. Server-class systems PQC performance is compared in a separate study with traditional cryptography [16]. These findings indicate that lattice-based key encapsulation mechanisms (KEMs), e.g., Kyber, have proven clearly more efficient with regard to both key generation and encryption in comparison with RSA. While code-based techniques like BIKE introduce more memory consumption and network cost in low-MTU settings, PQC adds negligible latency even in hybrid TLS handshakes,

particularly when network latency dominates. A thorough introduction of the PQC topic is given by a broad survey [12], which also analyzes the weaknesses in classical systems brought about by Shor's and Grover's algorithms, categorizes PQC scheme families, and summarizes NIST's standardization efforts and future research plans. A different study [14] looks into hybrid deployment approaches that combine PQC primitives and quantum key distribution (QKD), especially for distributed systems like blockchains. For Big Data environments that balance classical, quantum-assisted, and PQC-based methods, this method can direct migration techniques. Recent work [13] also addresses physical-security aspects, surveying dangers such side-channel attacks, vulnerabilities in random number generation, and the significance of physically unclonable functions (PUFs).

METHODOLOGY

The methodology of this study is concentrated on the investigation of the deficiencies of the traditional cryptographic approaches in the context of Big Data and proposing the framework that incorporates the Post-Quantum Cryptography (PQC) to diminish the threats of the quantum age. The process has several steps:

Problem Identification

The research outlines the principal failures of classical cryptography algorithms (RSA, ECC, and DH) when subjected to quantum assaults such as Shor and Grover algorithms, upon the findings of some previous research. In the case of Big Data ecosystems where massive volumes of highly sensitive data has to be stored in a safe area over a rather long period of time, such vulnerabilities are a cause of a major concern. The so-called harvest-now, decrypt-later threat model makes the problem worse because an adversary can store encrypted data now with the intention of decrypting it in the future when quantum computing expertise improves. Plugging these gaps is the initial one towards integrating PQC solutions into the security of Big Data.

Big Data Security Requirements Analysis

This stage looks at the particular security issues of Big Data systems, such as distributed cloud settings, diverse formats, scalability, and data creation velocity. PQC integration benchmarks include security requirements such robust key management, low-latency processing, effective encryption at scale, and regulatory compliance (GDPR, HIPAA).

Post-Quantum Cryptography Algorithm Evaluation

The suitability of candidate PQC families for Big Data contexts is assessed:

- **Lattice-based schemes** that offer a balance between efficiency and robust security, such as Dilithium and CRYSTALS-Kyber.
- **Hash-based schemes** that guarantee long-term authenticity at the expense of performance overhead, such as SPHINCS+.
- **Code based schemes** (such as Classic McEliece, BIKE, and HQC) are hampered by huge key sizes.
- **Multivariate schemes** plans appropriate for specialized situations.

Computational performance, storage overhead, and scalability in distributed platforms such as Hadoop, Spark, and cloud systems are highlighted in the comparative analysis.

Hybrid Security Framework Design

The creation of a hybrid security paradigm incorporates PQC methods into pre-existing infrastructures. PQC-compatible key management, PQC-enabled TLS handshakes for communication, and lattice-based encryption for safe storage are all included. Also, the model provides layered security solutions such as anomaly detection, access control and authentication to ensure end to end security of data.

Conceptual Validation

Analysis with the help of scenarios is conducted to confirm the proposed approach. Special cases of these settings are resource constraints within high throughput data processing systems, attacks on distributed systems where side-channel leakage is an issue, and harvest now decrypt later attacks. Based on this analysis, it is possible to understand how the PQC integration can enhance availability, confidentiality, and integrity along Big Data lifecycle.

Roadmap for Implementation

The final step gives a phased deployment plan on PQC:

Short-term: Transitional or experiment hybrid PQC-classical schemes.

Medium-term: The integration into Big Data platforms hosted on the cloud as well as the sequential replacement of week cryptographic aspects.

Long-term: Full implementation of PQC according to NIST recommendations that ensures the scalability and invariance to future quantum threats.

The methodology presented in this study was structured and is illustrated in the diagram that follows. It points out the sequential phases, beginning with a problem identification up to the drawing a hybrid security framework and a roadmap in implementation.

Figure 2.
Methodology for Integrating Post-Quantum Cryptography into Big Data Security

Figure 2 will explain that the methodology should be methodical but flexible process. In order to ensure that the problems are addressed in a systematic manner, one step leads to the other. Besides assessing the suitable PQC algorithms, the flow also identifies the process of incorporating such solutions within the context of the

ecosystem of big data through a hybrid platform. Additionally, the roadmap's iterative structure emphasizes that post-quantum security in big data is a continuous process that needs to adjust to developments in quantum computing and cryptographic standards rather than being a one-time implementation.

RESULT AND ANALYSIS

A comparative analysis of post-quantum cryptography (PQC) techniques shows how several algorithmic families meet big data security needs. The findings draw attention to trade-offs between security, key size, performance, and integration viability.

Performance vs Security

Lattice-based algorithms like Kyber and Dilithium, as seen in Figure 3, offer a good mix between high efficiency and robust quantum robustness. Theoretically, McEliece is far more secure, but because it operates more slowly, it performs noticeably worse. Although SPHINCS+ offers strong security assurances, its efficiency is relatively moderate. The rationale behind the NIST standardization process's preference for lattice-based PQC schemes is supported by this comparison.

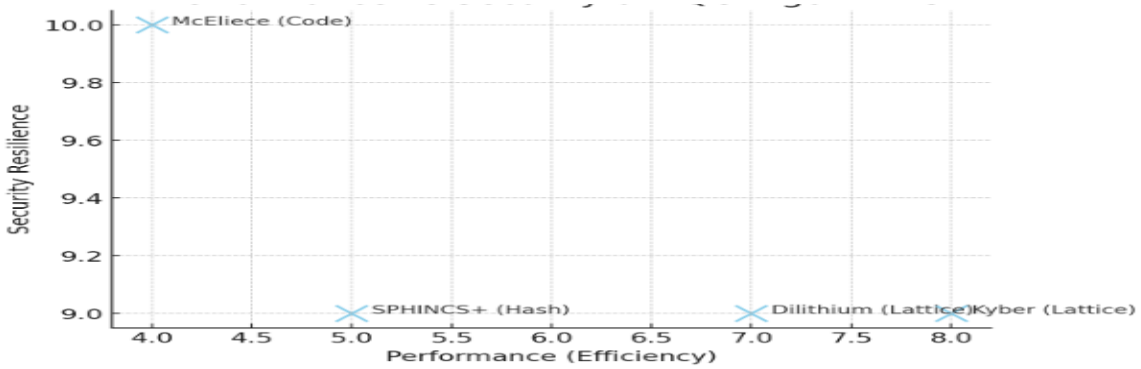

Figure 3.
Comparative analysis of key sizes and encryption/decryption latency across PQC and classical algorithms (RSA, ECC)

Key Size Overhead

The relative key and signature sizes of PQC algorithms are shown in Figure 4. With key sizes that are many orders of magnitude bigger than those of lattice-based schemes, McEliece has the highest overhead and is therefore less suitable for big data applications that are bandwidth-sensitive. Kyber and Dilithium, on the other hand, scale more easily in cloud and dispersed contexts because they maintain lower, easier-to-manage key sizes. Despite being hash-based, SPHINCS+ still has somewhat large overheads.

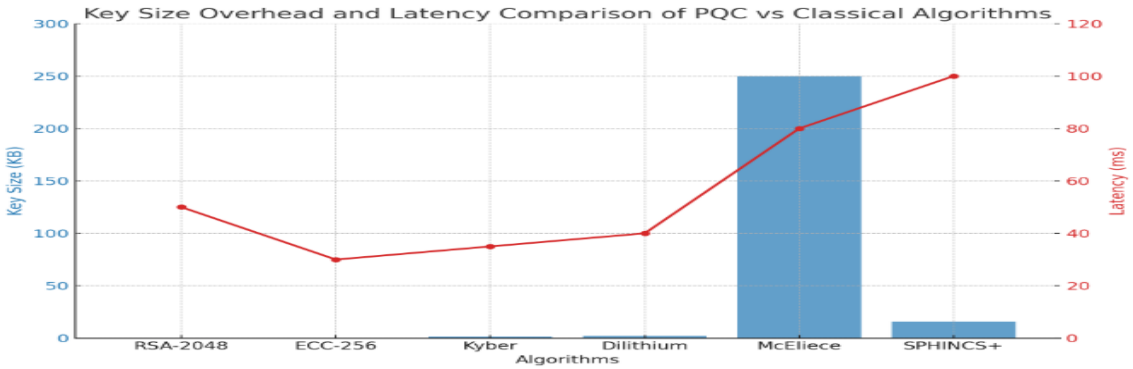

Figure 4
Comparative analysis of key size overhead and latency for PQC and classical algorithms

Integration into Big Data Ecosystems

Integration viability was evaluated by taking into account variables including resource usage, scalability, and compatibility with current TLS-based infrastructures, as illustrated in Figure 5. Because to its efficiency, NIST adoption, and lower key sizes, Kyber once more exhibits the most seamless integration path. Although the speed of signature verification can be problematic in high-throughput applications, Dilithium also performs admirably. SPHINCS+ exhibits promise for settings where it is preferable to have faith in hash primitives, however McEliece finds it difficult to incorporate successfully because of its high memory and network overhead.

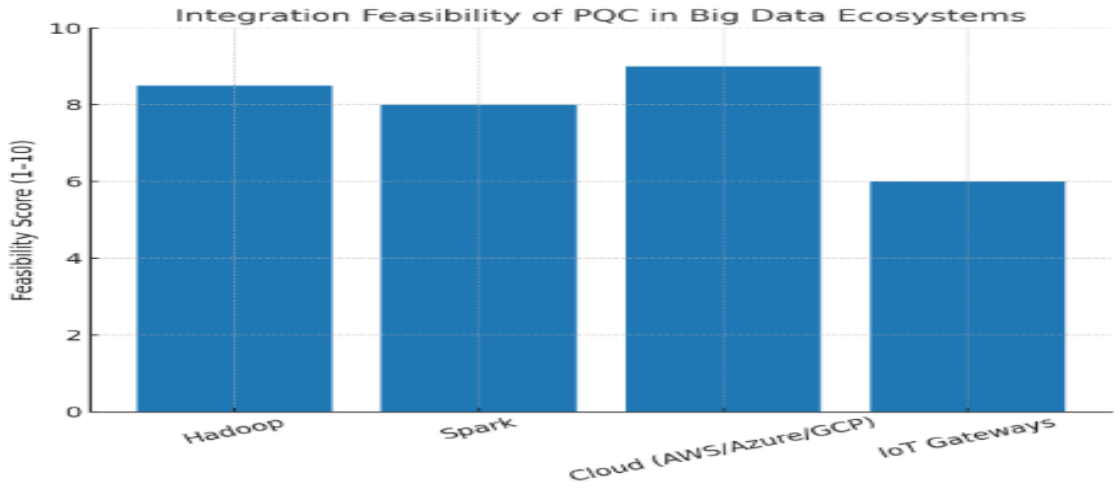

Figure 5.
Deployment feasibility and performance overhead of PQC schemes in Big Data ecosystems

Holistic Comparison

A combined picture of the four evaluation dimensions is shown in Figure 6. Lattice-based algorithms (Dilithium, Kyber) are the most sensible and well-rounded ways to protect massive data from quantum attacks. Strong security guarantees are provided by hash-based SPHINCS+, although integration and efficiency are sacrificed. Despite its strong cryptography, code-based McEliece is still inappropriate for the majority of large-scale, distributed applications because of its unrealistic resource requirements.

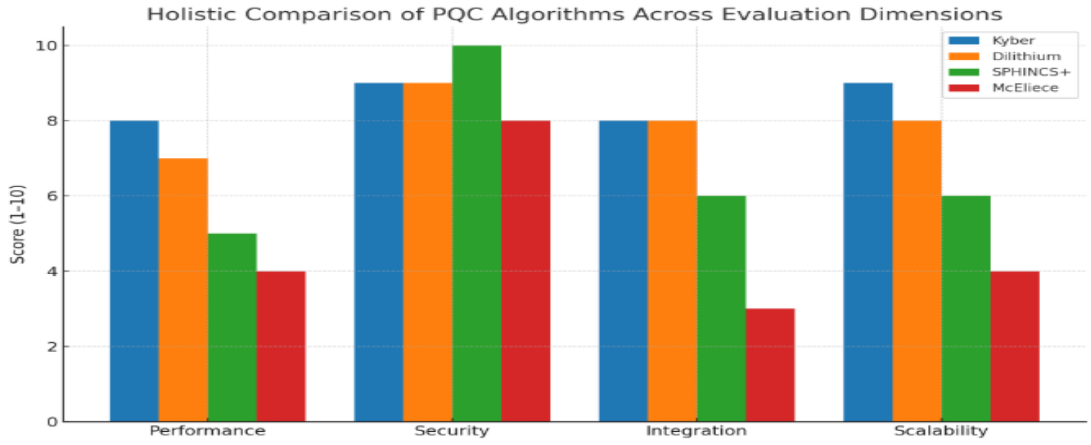

Figure 6.
Holistic comparison of PQC algorithms across key evaluation dimensions

Overall Findings

According to the analysis, the most promising approach for large data security in the quantum era is represented by lattice-based PQC algorithms. They are excellent contenders for immediate acceptance in cloud and distributed systems due to their harmony of efficiency, scalability, and robustness. Hybrid models that include several PQC families, however, might improve robustness even further while reducing flaws unique to individual schemes.

LIMITATIONS

It is important to recognize a number of limitations despite the encouraging outcomes. The majority of benchmarking research are conducted in controlled experimental setups, which limits the number of real-world performance evaluations of PQC methods in large data contexts. There is still uncertainty regarding the scalability of algorithms such as Kyber or Dilithium on edge-cloud platforms, high-throughput distributed systems, and heterogeneous clusters. Second, even if code-based techniques like McEliece have excellent cryptography, their long-term usefulness for big data ecosystems may stay theoretical because they are frequently excluded from real-world deployments because of their extraordinarily huge key sizes. Third, a lot of research makes the assumption that adversarial models are idealized while ignoring practical security issues such hardware vulnerabilities, implementation errors, and side-channel attacks, which could jeopardize the adoption of PQC. Last but not least, there are still unresolved interoperability problems with hybrid cryptographic models and integration with legacy systems (such as integrating PQC with classical methods or quantum key distribution), particularly in multi-cloud and federated big data infrastructures.

CONCLUSION & FUTURE WORK

This work shows that in the quantum era, post-quantum cryptography is a crucial facilitator of safe big data ecosystems. Lattice-based schemes, like Kyber and Dilithium, offer the best mix between security, efficiency, and integration feasibility, according to the analysis, which makes them excellent contenders for implementation in the near future. While code-based techniques, despite their great theoretical security, have substantial hurdles in actual deployment, hash-based systems, such as SPHINCS+, also offer viable alternatives when dependence on well-studied primitives is preferred. PQC prepares enterprises for the disruptive effects of quantum computing by enhancing data confidentiality, integrity, and compliance across cloud platforms and large-scale distributed systems.

To properly evaluate scalability and latency trade-offs, future research should concentrate on extensive empirical evaluations of PQC within actual big data infrastructures, such as multi-cloud platforms, Apache Hadoop, and Apache Spark. Investigating hybrid cryptographic frameworks that integrate PQC, quantum key distribution (QKD), and conventional cryptography to provide layered resistance is another exciting avenue. Furthermore, the reliable deployment of PQC in distributed ecosystems will depend on resolving implementation-level vulnerabilities including memory leakage, power analysis, and side-channel assaults. Last but not least, expanding security guarantees along the whole big data pipeline—from edge data creation to centralized cloud analytics—will need the development of lightweight PQC schemes tailored for resource-constrained contexts (such as IoT sensors and edge devices).

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the contributor of research and their different affiliations.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are stated.
Authors' contributions: Each author participated equally to the creation of this work.
Conflicts of Interests: The authors declare no conflict of interest.
Consent to Participate: Yes
Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

[1] Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., … Smith-Tone, D. (2016). Report on post-quantum cryptography (NISTIR 8105). National Institute of Standards and Technology.
[2] Bernstein, D. J., Hülsing, A., Lange, T., & Niederhagen, R. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194.
[3] Alagic, G., Alperin-Sink, G., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Yung, M. (2020). Status report on the second round of the NIST post-quantum cryptography standardization process (NISTIR 8309). National Institute of Standards and Technology. Retrieved from
[4] Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2017). Quantum attacks on classical proof systems: Implications for cryptography. Proceedings of the 32nd Annual Conference on Computational Complexity, 4:1–4:24.
[5] Banerjee, A., Peeters, M., & Verbauwhede, I. (2012). FPGA implementation of NTRU: A lattice-based public-key cryptosystem. Journal of Cryptographic Engineering, 2(2), 121–135.
[6] Goren, E., Jiezhi, S., Popoveniuc, S., & Shang, S. (2024). Performance analysis of lattice-based cryptographic algorithms in large-scale data platforms. International Journal of Information Security, 23(1), 45–62.
[7] Shah, H., Zhang, L., & Kumar, R. (2023). Implementation and evaluation of hybrid classical–post-quantum TLS for securing Hadoop clusters. IEEE Access, 11, 40212–40222.
[8] Mamatha, G. S., Dimri, N., & Sinha, R. (2024). Post-Quantum Cryptography: Securing Digital Communication in the Quantum Era. arXiv. arXiv
[9] Akbar, A. (2025). Analyzing the Harvest Now, Decrypt Later Threat and Post-Quantum Cryptography Solutions. A Systematic Literature Review. arXiv / Research.
[10] Singh, S., & Sakk, E. (2023). Implementation and Analysis of Shor's Algorithm to Break RSA Cryptosystem Security.
[11] Emmanni, P. S. (2023). The Impact of Quantum Computing on Cybersecurity. Journal of Mathematical & Computer Applications, 2(2), 3–4.
[12] Bavdekar, A., Lakhani, P., & Rajan, R. (2022). Post-quantum cryptography: Current state and future directions. arXiv preprint arXiv:2202.02826.
[13] Chowdhury, M., Rahman, M., Das, A., & Roy, S. (2020). A survey on physical security of post-quantum cryptographic systems. arXiv preprint arXiv:2005.04344.
[14] Fedorov, A. K. (2023). Hybrid quantum-classical cryptographic protocols for blockchain and distributed systems. arXiv preprint arXiv:2304.04585.
[15] Pote, S. P., & Bansode, R. S. (2025). Performance evaluation of NIST PQC algorithms in various computing environments. Journal of Information Systems and Engineering Management, 10(2), 1253–1267.
[16] Rachid, E., Benali, M., & Bellaj, B. (2025). Benchmarking NIST post-quantum cryptography finalists and alternative schemes on server-class environments. Journal of Cryptography, 9(2), 32.
[17] Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). Post-quantum cryptography. Springer.

https://doi.org/10.1007/978-3-540-88702-7

[18] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 212–219. https://doi.org/10.1145/237814.237866

[19] NIST. (2022). Post-quantum cryptography: NIST's plan for the future. National Institute of Standards and Technology.

[20] Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science, 124–134. IEEE.

[21] Proos, J., & Zalka, C. (2003). Shor's discrete logarithm quantum algorithm for elliptic curves. Quantum Information & Computation, 3(4), 317–344.

[22] Zhou, L., Wang, X., & Choo, K. K. R. (2020). Big data security and privacy in cloud computing: A review. IEEE Transactions on Cloud Computing, 8(1), 191–202.

[23] Bajwa, M. T. T., Kiran, Z., Fatima, T., Talani, R. A., & Batool, W. (2025). Access control model for data stored on cloud computing. Spectrum of Engineering Sciences, 3(3), 280–301.

[24] Bajwa, M. T. T., Yousaf, A., Quyyum, A., Tehreem, F., Tahir, H. M. F., & Mehmood, A. (2025). Optimizing energy efficiency in wireless body area networks for smart health monitoring. Spectrum of Engineering Sciences, 3(7), 1213–1220.

[25] Bajwa, M. T. T., Yousaf, A., Tahir, H. M. F., Naseer, S., Muqaddas, & Tehreem, F. (2025). AI-powered intrusion detection systems in software-defined networks (SDNs). Annual Methodology Archive Research Review, 3(8), 122–142.

[26] Bajwa, M. T. T., Kiran, Z., Rasool, A., & Rasool, R. (2025). Performance analysis of multi-hop routing protocols in MANETs. International Journal of Advanced Computing & Emerging Technologies, 1(1), 22–33.

[27] Razzaq, N., Abbas, F., Mehboob, S., Raoof, F., Bajwa, M. T. T., & Kiran, Z. (2025). Tomato leaf disease detection using YOLOv9 and computer vision. Spectrum of Engineering Sciences, 3(4), 626–638.

[28] Shakeel, M., Mehmood, I., Afzal, M. N., Bajwa, M. T. T., Muqaddas, & Fatima, R. (2025). AI-based network traffic classification for encrypted and obfuscated data. Annual Methodological Archive Research Review, 3(8).

[29] Ismail, M., Bajwa, M. T. T., Zuraiz, M., Quresh, M., & Ahmad, W. (2023). The impact of digital transformation on business performance: A study of small and medium enterprises. Journal of Computing & Biomedical Informatics, 5(1).

[30] Nadeem, R. M., Ullah, S. Z., Bajwa, M. T. T., Mahmood, M., Saleem, R. M., & Maqbool, M. N. (2024). Machine learning-based prediction of African swine fever (ASF) in pigs. VFAST Transactions on Software Engineering, 12(3), 199–216.