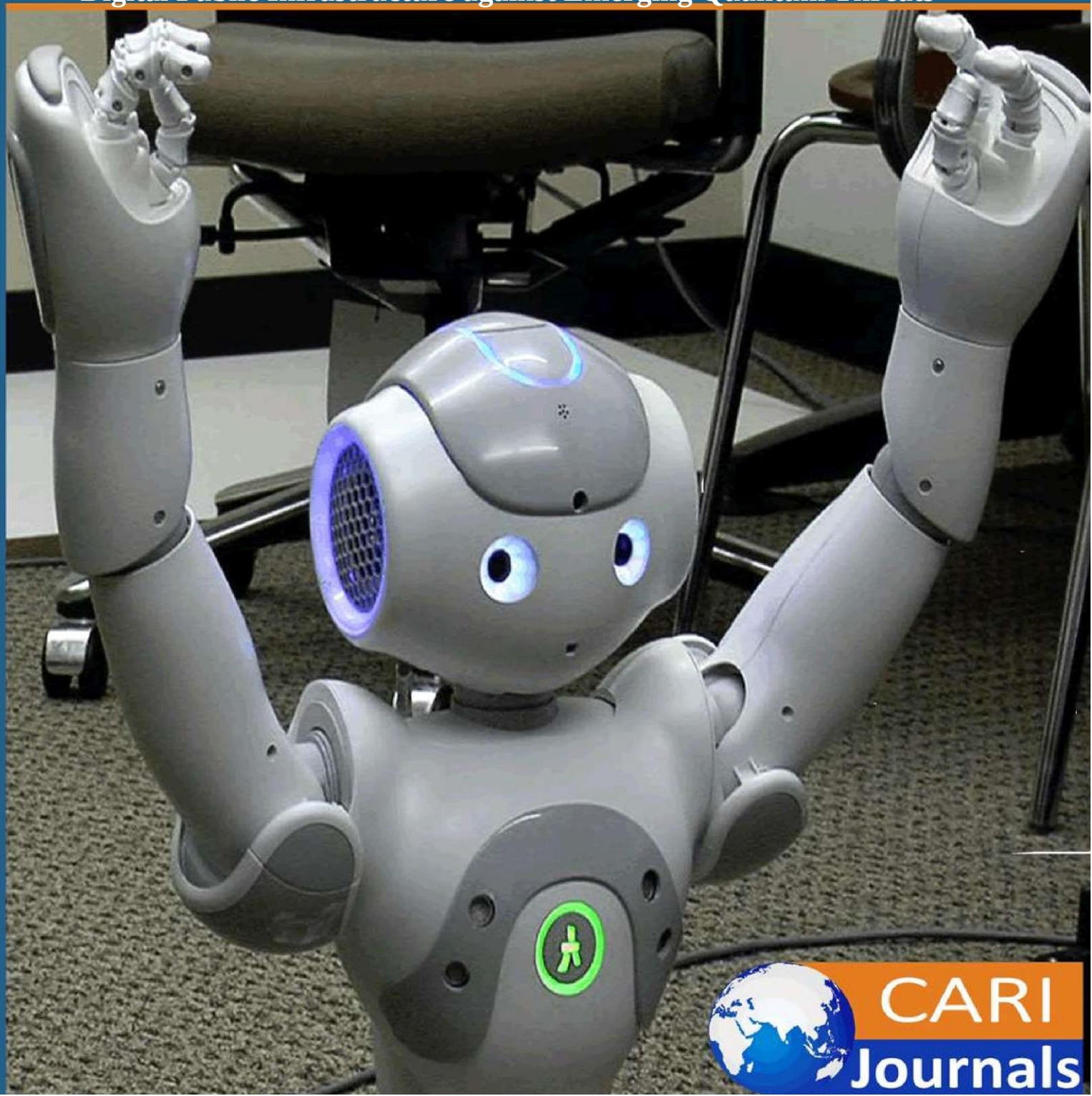
International Journal of
Computing and
Engineering
(IJCE)

Post-Quantum Cryptographic Framework for Securing Critical Digital Public Infrastructure against Emerging Quantum Threats



CARI Journals

International Journal of Computing and Engineering
ISSN 2958-7425 (online)
Vol. 8, Issue No. 2 pp 72 – 97, 2026
www.carijournals.org

Post-Quantum Cryptographic Framework for Securing Critical Digital Public Infrastructure against Emerging Quantum Threats

Dr. Abdinasir Ismael Hashi[1*], Mr. Osman Abdullahi Jama[2]

[1,2]Somali National University

https://orcid.org/0009-0009-0635-2609

Accepted: 5th May, 2026, Received in Revised Form: 12th May, 2026, Published: 23rd May, 2026

Abstract

Purpose: This study presents a comprehensive post-quantum cryptographic framework designed to secure Critical Digital Public Infrastructure (DPI) against emerging quantum computing threats.

Methodology: As traditional cryptographic methods become increasingly vulnerable, the proposed framework integrates post-quantum algorithms, hybrid cryptographic models, and a multi-layered architecture to ensure long-term data protection. The system is evaluated using key performance metrics such as latency, throughput, energy consumption, overhead, key size, and security strength. Additionally, an algorithm selection strategy is implemented to identify optimal cryptographic techniques.

Findings: Simulation results demonstrate that classical models offer better efficiency, while post-quantum approaches provide stronger security at the cost of higher resource usage. The hybrid model effectively balances these trade-offs, delivering improved security with moderate performance impact.

Unique Contribution to Theory, Policy and Practice: Overall, the framework provides a scalable, adaptable, and future-ready solution for protecting critical infrastructure in a rapidly evolving digital and quantum landscape.

Keywords: *Post-Quantum Cryptography, Digital Public Infrastructure, Hybrid Cryptography, Quantum Security, Algorithm Selection*

1. Introduction

The fast digitalization of the government, financial, health, and communication infrastructure resulted in the advent of "Critical Digital Public Infrastructure (DPI)" as one of the keystones of contemporary societies [1]. Digital Identity Platforms, Payment Gateways, E-Governance Portals, and Health Data Exchanges Serve 100s of Millions of People world-wide and would Help To Deliver Their Services Efficiently and Grow Economies Through These Services. Nevertheless, this growing dependence on the interrelated digital ecosystems has also increased the threat of cybersecurity attacks [2]. The most notable of these is the introduction of quantum computing which is a paradigm-shifting threat, one that can weaken the cryptographic primitives that currently secure DPI [3]. Figure 1 illustrates the main categories of "Post-Quantum Cryptography (PQC)". The central node represents PQC, surrounded by four key approaches: lattice-based, code-based, hash-based, and multivariate cryptography. Each category uses different mathematical techniques to provide security against quantum attacks, collectively forming a robust foundation for quantum-resistant systems.

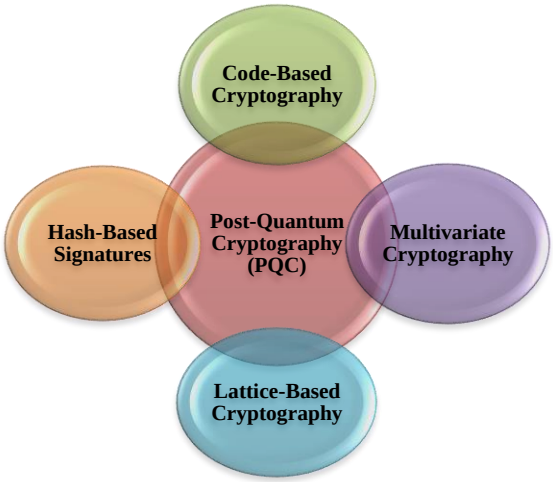


Figure 1: *Classification of Post-Quantum Cryptographic (PQC) Algorithms*

Modern cryptographic protocols (including popular public-key algorithms such as RSA and "Elliptic Curve Cryptography (ECC)" use the fact that mathematical problems like integer factorization and discrete logarithms are computationally infeasible [4]. Although these assumptions are solid in comparison to the classical computing capabilities, quantum algorithms, most notably those of Shore are a threat to the strength of such algorithms by providing solutions to such problems efficiently [5]. This means that sensitive data that is encrypted today can be attacked in the near future, a phenomenon commonly known as the harvest now, decrypt later attack model. The risk is especially vital to DPI where the confidentiality, integrity, and trust of long-term data are fundamental [6].

PQC has become an important target solution in response to these emerging threats. PQC is a type of cryptographic algorithm that is secure against classical and quantum adversaries [7]. PQC is a convenient and scalable method to securing current infrastructure, compared to quantum cryptography, which uses quantum mechanics, and can be deployed on existing classical systems. Efforts outside the U.S. have boosted the creation and testing of quantum-resistant algorithms, including lattice-based, hash-based, code-based, and multivariate polynomial cryptosystems [8-10].

This proposed study would outline a Post-Quantum Cryptographic Framework to defend Critical Digital Public Infrastructure against the emerging quantum threats. The proposed framework comprises of a multi-layered and modular structure, utilizing quantum-resistant algorithms, hybrid cryptography schemes, key management and secure, continuous risk evaluation [11]. Additionally, practical implementation considerations like scalability, interoperability, and changing standards would be considered. Lastly, the proposed framework would bridge the divide between theory and implementation in addressing the practical aspects of using cryptographic resiliency to support DPI [12].

In addition, this study describes a requirement for a crypto-agility strategy that provides the capability for systems to be able to adapt their cryptographic standards dynamically as the risk landscape continues evolving. Risk-based criteria were also implemented within the framework, so that an organization can determine which of its most critical assets require higher levels of security within their DPI [13]. This would allow organizations to provide an incremental, secure migration approach to a post-quantum world without adversely impacting their existing services. This study provides a necessary holistic view of both technology innovation and the strategic implementation needed. With governments and organizations worldwide investing in digital transformation, the need for long-term protection for any organization's DPI is paramount. A lack of proactive management of quantum threats could result in severe repercussions, including data breaches and/or lost trust in the public and systemic disruptions [14].

This study was conducted in a careful and deliberate way to help answer the study question(s). The introduction provides information about what led to this study and why it is important. The literature review is an overview of studies and provides an analysis of existing literature to determine what previous researchers have found as well as to identify research gaps. The methodology section explains how to create a post-quantum cryptography framework based on proposed methodologies. The results and discussion sections provide evaluations of the framework's performance and implications in practice (i.e., how it would be used). The main Objectives of the study are as follows:

- To analyze the vulnerabilities of existing cryptographic systems within Critical Digital Public Infrastructure in the context of quantum computing threats.

- To evaluate and compare various Post-Quantum Cryptographic algorithms suitable for large-scale DPI deployment.
- To design a comprehensive and scalable PQC-based security framework tailored for diverse DPI environments.
- To assess the performance, interoperability, and implementation challenges associated with integrating PQC into existing systems.
- To propose strategies for crypto-agility and phased migration to ensure a secure transition to quantum-resistant infrastructure.

2. Literature Review

Recent studies on PQC-related work to secure CDPI that include the study proposed was by **Majumder et al. (2026)** [15], which identified a lack of preparedness for the post-quantum adoption of PQC as a primary roadblock to its widespread use. The study recommended using hybrid PQC models, along with policies to aid adoption; the results suggested that the level of awareness of PQC relates strongly to its adoption. **Shirisha et al. (2026)** [16] proposed lightweight lattice-based cryptographic techniques to optimize resource usage for energy and latency in their investigation of resource constraints. **Devaraj et al. (2026)** [17] proposed a multi-tiered post-quantum cryptography solution for 6G health systems to improve data security and reduce information transmission delays. At the same time, **Jamolova et al. (2026)** [18] developed a quantum-safe system through the combination of post-quantum cryptography and quantum key distribution for financial systems, while **Olisa et al. (2026)** [19] evaluated CBDCs based on the interoperability of post-quantum cryptograph standards. All of the previously mentioned studies employed simulation, statistics and experimentation as methods of study and achieved quantum resistance at the expense of high resource costs. After the work was concluded, performance-based investigations were done. **Faval, et al. (2026)** [20] examined the use of post-quantum cryptography (PQC) in a 5G Core Network and reported that it provided acceptable latency, while **Kannan, et al. (2026)** [21], developed the Q-EDGE-OS which demonstrated successful implementation of low-latency PQC on IoT devices. Lastly, **Rassekhnia, et al. (2026)** [22], created a Quantum Encryption Resilience Score (QERS) to evaluate the effectiveness of PQC with respect to platform performance and security. All of these papers demonstrate feasibility using benchmarking, simulation, and real-world implementation, but each has limitations specifically, overheads associated with the implementation of PQC.

The order of discussion about application-driven frameworks is sequentially presented. **Khan et al. (2025)** [23] proposed a blockchain-supported PQC framework based on zero knowledge proof validation, which verifies authenticity and ensures resiliency through high levels of data integrity with reduced levels of vulnerability. Conversely, **Balogun et al. (2025)** [24] researched the inclusion of PQC within telemedicine and determined that the Falcon algorithm was the most

effective, though there are still identifiable vulnerabilities within the distributed ledger system. **Reddy et al. (2026)** [25] constructed QuantumShield-BC - A PQC framework built on Blockchain technology, possessing resistance against quantum computer attacks, whilst also providing a high volume of service capability. **Meenalochini et al. (2025)** [26] determined a lightweight solution for an Internet of Things-based key exchange protocol using PQC. All study results relied on either experimental data, or statistical analysis to establish results. **De Haro Moraes et al. (2024)** [27] proposed a CBDC architecture based on PQC providing excellent security with outstanding performance featuring distributed ledger and trusted execution mechanism characteristics. Finally, **Scalise et al. (2024)** [28] supplemented this sequence by evaluating the effect of implementing PQC into 5G Networks; noting minimal impacts on latency and bandwidth, but drastically enhancing security characteristics. In addition to offering clear and objective evidence of the criticality of PQC for future-infrastructure security, this set of consecutive literature sources from [15]-[28] demonstrates the continuing problems with scalability and performance that can be associated with using PQC.

3. Research Methodology

This study uses a design science and system-oriented approach to create a strong Post-Quantum Cryptographic Framework to secure the Critical Digital Public Infrastructure (DPI) from new quantum risks. The design incorporates system modeling, a complete threat assessment process, designing of a framework architecture, the choice of post-quantum algorithms, and the analysis of the different frameworks' performance using multiple criteria. By integrating theoretical principles with practical implementation issues, the methodology ensures that the framework being recommended would be both: a cryptographic obstacle for quantum adversaries; and would be scalable, interoperable and capable of being implemented in multiple types of DPI environments.

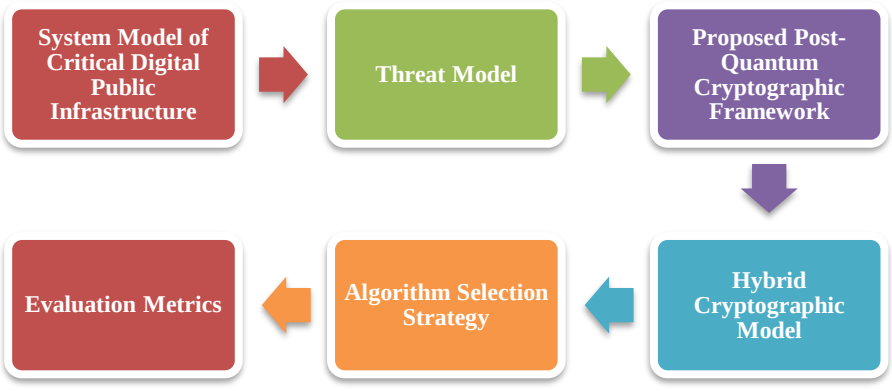


Figure 2: *Framework of Proposed Methodology*

3.1 System Model of Critical Digital Public Infrastructure

Digital Public Infrastructure, EPI system design employs an integrated: 3-tiered: app, net & sec; approach. Each of these three layers is integrated together and work in conjunction with one another to provide an end-to-end solution for successful & secure digital services [29]. App Layer: This is comprised of apps that provide service delivery & transactional functions such as Identity (e-ID), Payment (fiat & non-fiat), Health (HIS), e-Gov (MDG) etc. Net Layer: This provides communication via cloud, edge, and next gen networks (5G/6 G) technologies [30]. Sec Layer: Includes mechanisms to perform cryptography, auth, key mgmt.- each sec mechanism protects based on confidentiality, integrity, availability, and resilience to classical & quantum threats [31].

- **Application Layer (L_A)**

The Application Layer (L_A) comprises the service-based elements of DPI, which include digital identity solutions, payment/financial solutions, healthcare databases, and e-governance applications. This layer can be defined as follows:

$$L_A = \{A_1, A_2, A_3, A_4\} \quad (1)$$

Every application deals with confidential data $D_i = \{d_1, d_2, \ldots, d_n\}$, making it imperative to provide robust security measures for the application layer. Security needs for this layer are specified as:

$$Security(L_A) = Confidentiality + \text{Integrity} + \text{Availability} \quad (2)$$

It is crucial that this layer ensures the proper processing and access control because of its direct interaction with users and sensitive data.

- **Network Layer** (L_N)

Distributed DPI constituents communicate and transmit data over the network layer, which consists of (1) Cloud Infrastructure, (2) Edge Devices, and (3) Communication Networks (e.g., 5G/6G). Below is a definition of the network layer.

$$L_N = \{N_C, N_E, N_T\} \quad (3)$$

Using the data carried by the network layer, the data transmitted across a network appears as follows:

$$T(D): L_A \rightarrow L_N \rightarrow L_A \quad (4)$$

The effectiveness and efficiency (or performance) of this layer's transmission medium (or method of communication) is evaluated using the following metrics:

$$Performance(L_N) = f(Latency, \text{Bandwidth}, \text{Throughput}) \quad (5)$$

Intercommunication throughout this layer is critical to achieving low-latency, highly available, and dependable service delivery.

- **Security Layer** (L_S)

With respect to both classical and quantum threats, the Security Layer (L_S) provides protective mechanisms. The Security Layer (L_S) can be described as:

$$L_S = \{C, A, K\} \quad (6)$$

Where C represents any/each of the existing cryptographic mechanisms; A refers to the different Authentication Systems available for use; refers to any Key Management technique. The Security Functionality can be described as:

$$Security(L_S) = \text{f}\ (C_{PQC,} A, K) \quad (7)$$

For the purposes of this document, C_{PQC} refers to the various Post-Quantum Cryptographic algorithms. The overall purpose of the Security Layer L_S is to provide secure transmission, secure access control, and secure Key Distribution across all implementations of a Critical Digital Public Infrastructure system and provide the framework for building Quantum-Resilient Security within Critical Digital Public Infrastructure.

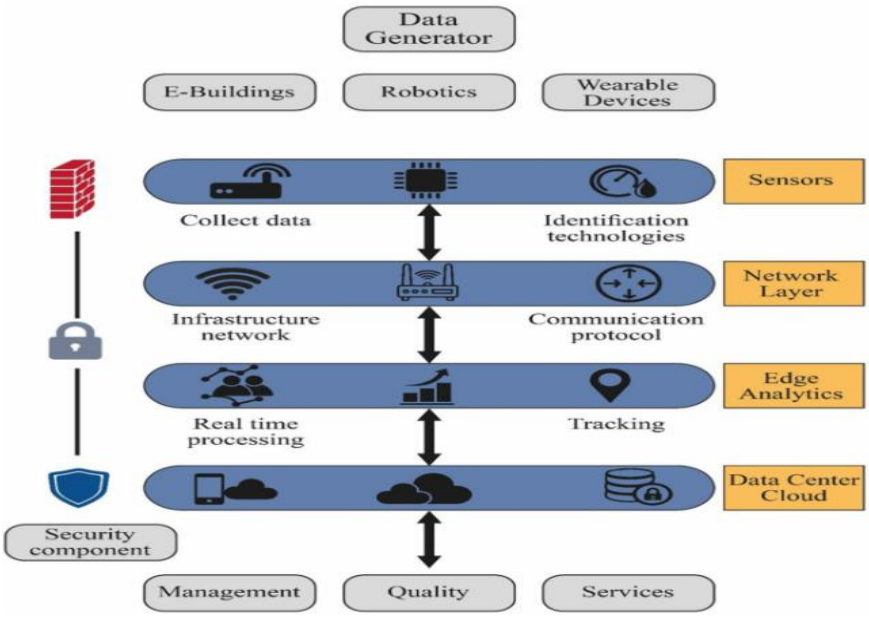


Figure 3: *System Model of Critical Digital Public Infrastructure (DPI) [32]*

3.3 Threat Model

This study provides a Verifiable Threat Model for evaluating the potential security threats of Quantum Computing against the overall Threat Vulnerability of all Critical Digital Public Infrastructure Systems. All security risks to PII (protected Innovation Information) based on the

use of Classical Cyber Combat Systems have been analysed, including those security risks associated with the advanced computing abilities of adversary forces and the implementation of Quantum Computers to conduct attacks against Critical Digital Public Infrastructure systems.

$$T = \{T_Q, T_H, T_S\} \quad (8)$$

Where T_Q represents Quantum Threats, T_H represents Harvest-Now-Decrypt-Later attacks, T_S represents System Level Threats. By structuring threats within a Threat Model; studies are developing a post-quantum Cryptographic Framework that would provide Long Term Security and Resilience for Critical Digital Public Infrastructure Systems.

- **Quantum Adversary** (T_Q)

The quantum adversary model postulates the existence of attackers with access to quantum computing power, who can exploit Shor's algorithm to compromise classical cryptographic algorithms, such as RSA or ECC. The level of vulnerability can be expressed mathematically as:

$$Security_{classical} \to 0 \; as \; Q \to \infty \quad (9)$$

Where Q = quantum computing power. Adversaries using quantum computers would easily solve the problems of integer factorization and discrete logarithms, thus compromising encryption, authentication, and key exchange. As such, the threat of quantum computing would greatly reduce the confidentiality of long-term data stored within Data Privacy Impact (DPI) systems unless there is a transition to "quantum resistant" cryptographic algorithms.

- **Harvest-Now-Decrypt-Later (HNDL) (T_H)**

As a separate but related concern, attackers may use the HNDL (holds and decrypt later) attack model to collect and store today's encrypted data, with the intention of decrypting it once quantum computing becomes a reality. The HNDL attack may be represented mathematically as:

$$D_{future} = Decrypt_{quantum}(Encrypt_{today}(D)) \quad (10)$$

This threat is especially significant to DPI systems, where long-term sensitivity of data is a concern (e.g., medical records and financial records). While today's encryption may be secure against current attack methods, in the future, quantum computing may expose all stored data. Therefore, the proactive adoption of post-quantum cryptography is critical to mitigating the risk of delayed decryption.

- **System-Level Threats (T_S)**

The types of threats to system-level (cybersecurity) include the following: (1) typical cyber-attacks (e.g., malicious insider), (2) data tampering, and (3) theft or interception of communications. Each of these threats can be expressed as follows:

$$T_S = \{T_{insider}, T_{tamper}, T_{intercept}\} \quad (11)$$

(1) Insider attacks are generally attacks on integrity by trusted parties, (2) Tampering with the data is an attack on integrity (3) Interception of the message compromises confidentiality during the delivery of such information. While all three attacks can occur independently of quantum capabilities, it is possible for them to be magnified when studies occur in a distributed Critical Digital Public Infrastructure (DPI) environment. Therefore, the use of robust authentication, secure communication protocols, and monitoring systems should be utilised in addition to the post-quantum cryptography.

3.4 Proposed Post-Quantum Cryptographic Framework

The framework presented is a layered, modular architecture for the design of Critical Digital Public Infrastructure (DPI) that provides scalability, flexibility, and quantum-resilience. The framework is made up of integrations of (1) cryptographic functions, (2) key management, (3) access control, and (4) monitoring components into a single system that can be expressed as follows:

$$F_{PQC} = \{L_C, L_K, L_A, L_M\} \quad (12)$$

Where L_C is the cryptography layer, L_K is the key management layer, L_A is the access control layer, and L_M is the monitoring layer. With this overall structure, the features of (1) securing communication, (2) efficient management of keys, (3) controlling access, and (4) detecting threats in real time from traditional or quantum attacks, would be accomplished.

- **Cryptographic Layer (L_C)**

The cryptographic layer provides quantum-resistance in both encryption and signature algorithms, using lattice algorithms such as Kyber and Dilithium, hash-based signatures such as SPHINCS+, and hybrid cryptographic methods of combining traditional and PQC methods. The security function is defined as:

$$C_{total} = C_{classical} + C_{PQC} \quad (13)$$

Where C_{PQC} can provide protection against quantum-based attacks. Hybrid cryptography provides an ability to maintain backward compatibility as studies are transitioning to quantum-safe systems. This layer provides the framework with the confidentiality, integrity and authentication protections necessary for the foundation of the framework's resilience against the threats posed by emerging quantum computing.

- **Key Management Layer (L_K)**

The key management layer provides for the secure generation, distribution, storage and renewals of cryptographic keys. This layer uses the Post-Quantum Key Encapsulation Mechanics (KEMs) such as Kyber to provide secure key exchange. The lifecycle of the key can be defined as:

$$K_{life} = \{k_{gen,}\, k_{dist,}\, k_{use,}\, k_{update,}\, k_{revoke}\} \quad (14)$$

This layer would provide key confidentiality and integrity across the distributed DPI systems. Efficient key revocation and rotation methods would mitigate the risk of losing the confidentiality of the key and ensure long-term cryptographic security in a dynamic operational environment.

- **Access Control Layer (L_A)**

The access control layer uses Zero Trust Architecture (ZTA), multi-factor authentication, and identity-based access controls for secure authentication and authorisation mechanisms. All access control decisions are defined as:

$$Access = f(Identity, Authentication, Authorization) \quad (15)$$

Zero Trust architecture assumes nothing, and everything needs to be validated for every access request continuously. Each layer in the architecture allows only those authorized users or systems to have access to sensitive DPI resources, significantly reducing the risk associated with unauthorized users accessing sensitive resources or becoming inside threats.

- **Monitoring and Risk Layer (L_M)**

The risk and monitoring layer would enable systems to continue to monitoring and detect possible threats to the systems continuously. Multiple analytical and detection capabilities exist within this layer, including anomaly detection, real-time monitoring of system activity, and risk ranking for critical assets. Risk analysis can be depicted as follows:

$$Risk = Probability \times Impact \quad (16)$$

The monitoring and risk layer accomplishes its goal of timely mitigation of anticipated vulnerabilities and threats by proactively identifying possible threats and vulnerabilities and leveraging continuous monitoring and analysis of suspected compromise of systems and ranking of vulnerable critical assets. The overall security posture of DPI systems would increase while staying on top of new threats, including potential attacks from quantum-computing technology.

3.5 Hybrid Cryptographic Model

To provide a seamless migration path from classical to post-quantum security mechanisms, hybrid cryptography would be utilized for backward compatibility. Through combining traditional cryptographic algorithms with post-quantum methodologies, all systems would maintain their secure operation until transitioning completely to quantum-resistant methodologies. This would minimize any disruption to existing infrastructure and would expand the interoperability between legacy and modern systems. The phased migration strategy associated with the hybrid model would provide layered protection to all sensitive data for both current cybersecurity threats and future risk associated with quantum computing.

3.6 Algorithm Selection Strategy

A post-quantum algorithm selection process is established based on standardized recommendations for securing systems. The selection considers the trade-offs of security strength, efficiency, key length and scaling capability. Kyber is appropriate for encryption, Dilithium for digital signature creation and SPHINCS+ for hashing mechanism based security protocols with balanced performance trade-offs between quantum resistant and speed.

Algorithm 1: Post-Quantum Cryptographic Algorithm Selection Procedure

```
Input: Set of candidate algorithms A = {a1, a2, ..., an}
       Selection criteria C = {Security, Efficiency, KeySize, Scalability}
Output: Selected algorithms S
Begin
  Initialize S ← ∅
  For each algorithm ai in A do
    Evaluate SecurityScore(ai)
    Evaluate EfficiencyScore(ai)
    Evaluate KeySizeScore(ai)
    Evaluate ScalabilityScore(ai)
    Compute OverallScore(ai) =
      w1*SecurityScore(ai) +
      w2*EfficiencyScore(ai) +
      w3*KeySizeScore(ai) +
      w4*ScalabilityScore(ai)
  End For
  Select top algorithms based on highest overall score
  Assign:
    Encryption ← Kyber
    Signature ← Dilithium
    Hash-based ← SPHINCS+
  S ← {Kyber, Dilithium, SPHINCS+}
  Return S
End
```

3.7 Evaluation Metrics

The performance of the framework is evaluated against many metrics that would yield quantitative measures of efficiency, scalability and security properties, using defined mathematical equations to create quantitative values per metric:

- **Latency (L):** $L = t_{enc} + t_{dec} + t_{comm}$ (17)
- **Computational Overhead (C):** $C = \frac{T_{total} - T_{base}}{T_{base}}$ (18)

- **Energy Consumption (E):** $E = \sum P_i \times t_i$ (19)
- **Key Size (K):** K=|Key| (bits) (20)
- **Throughput (T):** $T = \frac{N_{operations}}{t_{total}}$ (21)
- **Security Strength (S):** $S = log_2(Attack\ Complexity)$ (22)

Collectively these values from all metrics would be used to define a performance vector.

$P = \{L, C, E, K, T, S\}$ (23)

4. Result and Analysis

This section analyze results from simulations to provide an accurate understanding of the performance characteristics of various key metrics (including Latency, Throughput, Security and Resource Consumption) for different Cryptography Models. The Result further analyzes the performance of each model to determine which one provides the best trade-off between performance and security for real-world use.

4.1 3 – Layer DPI model

The Three-Layer DPI Model (Device-Platform-Interface) defines how digital systems are constructed on three levels: hardware, software platform, and layer of user interaction with the applications. By understanding how data flows through these systems, designers and engineers can gain a better understanding of how the components of their digital system would work well together and therefore would provide an efficient way to process data.

Figure 4 shows the latency values for each simulation run over the course of 50 runs. As can be seen from the data, there was significant variance in the latencies across the simulation runs. Minimum latency was approximately 6 seconds, maximum latency was approximately 26 seconds, and therefore, the latencies overall do not depict a consistent response by the overall system. In addition, most of the latencies were between 15 seconds and 23 seconds, and therefore this should be considered as the practical range of typical operations for this system. The majority of the simulation runs with sharp drops in latency occurred around run numbers 8, 12, 21, 35 and 41, with latencies below ten seconds. In contrast, there were a number of simulation runs with latency spikes above 24 seconds, including runs 3, 22, 37 and 43. The overall latencies in the results do not consistently trend in either an upward or downward fashion, thereby indicating that the performance was affected predominantly by randomness rather than through gradual improvements or degradation of performance over time.

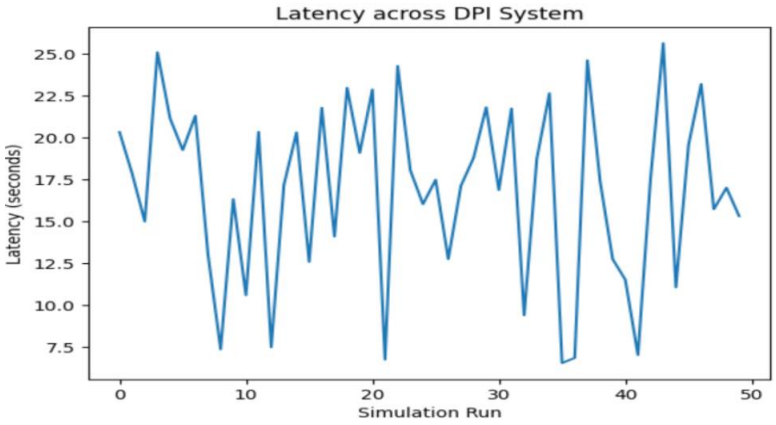


Figure 4: *DPI system latency across simulation runs.*

Figure 5 represents the DPI performance with multiple simulations performed on the system to illustrate its ability to effectively process data through a sequence of time intervals. Throughput speeds are consistently high, specifically between 91 and 99 Mbps. Most of the throughput values would reflect mid-range (i.e., approximately 94-96 Mbps). Therefore, it can be concluded that the DPI System is stable and reliable, with minor variation in throughput speeds, or even a small number of throughput dips and throughput peaks would not have a significant impact on the overall performance of the DPI system. Variability in throughput speeds can be attributed to a wide variety of reasons including differences in processing power and/or different conditions on the network, as there would be variations between each run of the simulation. In summary, the DPI system demonstrates continued reliability and consistency in throughput speed, which allows for continuous and high-volume data-processing operations to take place.

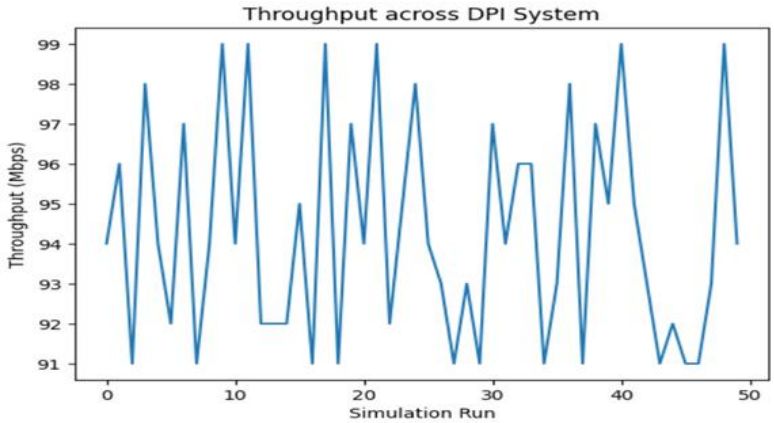


Figure 5: *Throughput performance of the DPI system across multiple simulation runs.*

4.2 Threat Model

Threat modeling is a process for identifying potential security risks associated with a proposed or existing application, including what attackers and/or vulnerabilities exist. Once these elements

have been identified, a threat model would be developed that would assess alternative attacks on the identified application and develop alternatives to mitigate those threats by analyzing the various potential attacks.

Figure 6 presents the threat score values from the DPI simulation that fluctuate widely, with scores falling within the range 23-84; however, most of the scores are between 25-45. Thus, the scores suggest that most of the simulations would reflect a moderate threat level, and thus the majority of the simulations would reflect a moderate threat environment. Nevertheless, there are some significant spikes observed where the threat score exceeds 60; therefore, there are some periods of more pronounced risk (greater than average) or abnormal activity. Furthermore, these spikes do not occur regularly; therefore, high risk (high threat) events may occur sporadically versus continuously. The variation in the threat score may be due to how traffic patterns changed throughout the simulation period or how the attack simulations were performed. Overall, while the overall threat level is believed to be intermittent periods of high threat levels, for the majority of time period, the overall threat level reflects a stable and manageable threat level throughout the simulation period.

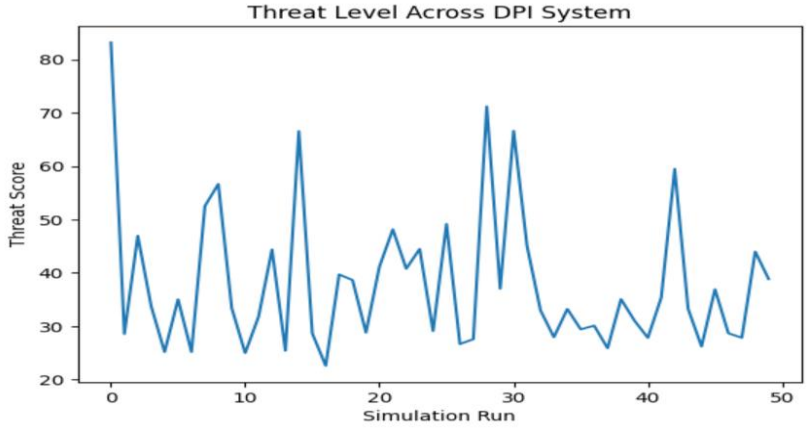


Figure 6: *Threat level variation across DPI simulation runs.*

4.3 PQC Framework

The PQC framework was developed for protecting systems from attack by quantum computers. It utilizes advanced cryptographic algorithms that have a longer useful life than traditional forms of encryption due to the expected vulnerability of the latter in the future. Figure 7 shows the observations of the PQC framework indicates that processing times vary among different simulations over the course of several runs. The average processing time for most observations is approximately between 9 and 13 seconds, indicating reasonably consistent processing performance, and the blocks of smaller 5 to 6 seconds and larger 17-18 seconds processing times are indicative of performance-related conditions caused by the processing of varying workloads during different runs. Overall, the PQC framework has consistently produced reasonable levels

of performance when operating under normal operating conditions, despite occasional minor variations, across a broad spectrum of simulation environments.

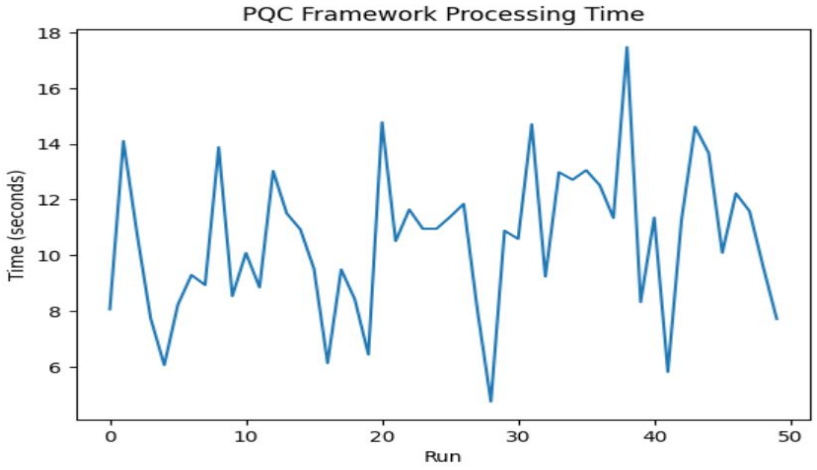


Figure 7: *PQC framework processing time across simulation runs.*

Figure 8 shows the binary outcomes of an access control that are produced from a large number of running programs and result in alternating allow (1) and deny (0) results. The pattern is dynamic with rapid transitioning between allowing access and disallowing access, and there is a very slight emphasis toward the allow outcome even though there are many instances of disallow being present, indicating strict enforcement of access policy. The irregular distribution shows that there is a constant evaluation of the ability to grant access based on fluctuating conditions rather than based upon fixed access rules.

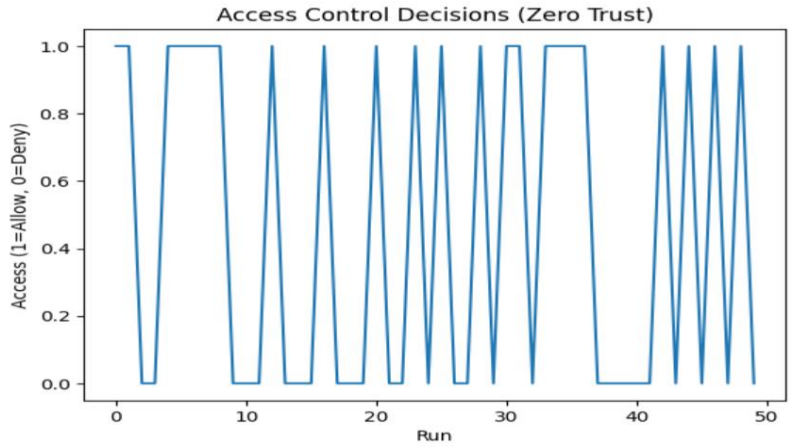


Figure 8: *Access control decisions under the Zero Trust model across simulation runs.*

Also the occasional pattern of clusters of consecutive allows or disallows indicates that there may have been times when allowing access or disallowing access behaved consistently for short periods of time. Overall, the results indicate that Zero Trust is a responsive access control

mechanism that provides realtime configuration of decisions while still maintaining the level of security required and provides legitimate access when warranted.

Figure 4.6 shows the level of risk monitoring varied greatly over a number of runs with most of the values falling somewhere between 0 and 10. The majority of values (scores) were concentrated in the mid-range of 4 and 8 indicating that there were an overall moderate level of risk for most of the observations, but from time to time there were periods of rapid change with very low risk (scores near 0) and very high risk (scores near 9 or 10). However there is a great deal of variance in how the system responded to changing conditions, hence the apparent high variability in the data makes it appear that the system was continually adapting to changing environmental conditions. The results suggest a dynamic environment characterized by generally moderate to low risk with occasional instances of elevated risk.

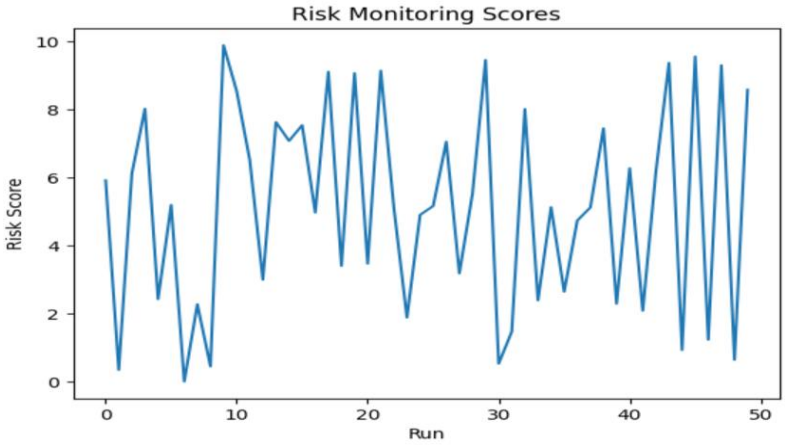


Figure 9: *Risk monitoring scores across simulation runs.*

4.4 Hybrid Cryptographic Model (Classical + PQC)

A hybrid cryptographic model (classical + post-quantum) provides increased security by incorporating classical encryption with post-quantum algorithms. A hybrid model is designed to strike a balance between performance and future-proof security. Figure 10 shows an average of 3 simulations that was completed for each of the three types of cryptographic approaches, and the classical model exhibited the lowest average latency (consistently between 1 and 3.5 sec.), indicating very fast processing. The post-quantum model exhibited periods of moderate latency (approximately 3 and 11 sec.) due to higher computational overhead resulting from longer running times. The hybrid model exhibited the highest period of latency (approximately 3 to 14 sec.) since the combination of classical and post-quantum crypto methods required extra time for execution. All three models did experience fluctuations in latency due to changes in the level of encryption used, but the overall performance of each remained relatively consistent through all simulations.

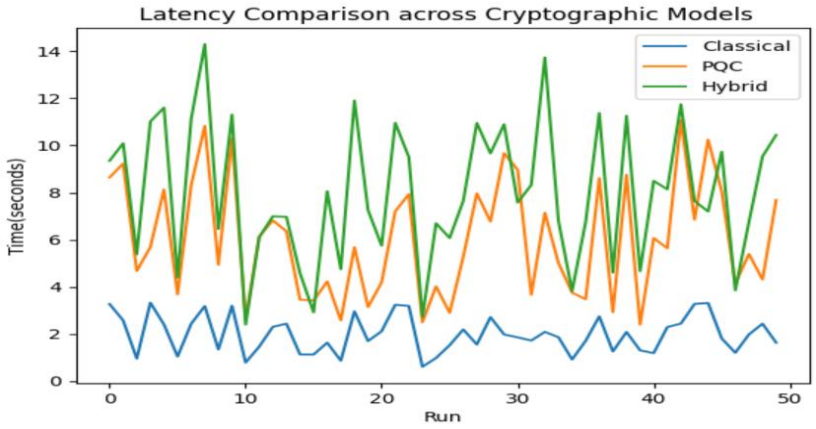


Figure 10: Latency comparison across classical, PQC, and hybrid cryptographic models.

Figure 11 shows various encryption techniques produce different results when tested for the level of security over an extended period of time. The classical encryption method had the lowest level of security, scoring around 3 to 5, indicating that classic techniques provide weaker security than other encryption methods. Conversely, PQC and hybrid encryption techniques score on average between 8 and 10, demonstrating significantly higher levels of security than classical methods. In addition, because hybrid techniques utilize both classical and PQC algorithms, it frequently achieve a score of nearly 10, demonstrating enhanced security compared to their individual counterparts. All three encryption techniques have experienced some minor fluctuations over time, but PQC and hybrid techniques continue to exhibit consistent levels of strength.

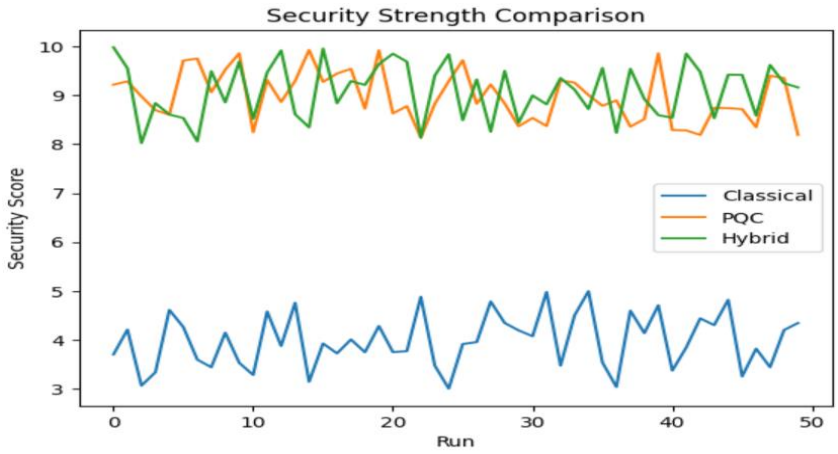


Figure 11: *Security strength comparison across classical, PQC, and hybrid cryptographic models.*

4.5 Algorithm Selection

Algorithm selection is the process of determining appropriate cryptographic algorithms for a system based on performance, security, and efficiency criteria. It allows for optimal balance

between strength of protection and cost of computation for different systems. Figure 12 shows the relative scores assigned to cryptographic algorithms based upon overall suitability. The prime choice of all those considered, Kyber scored approximately 7.8, which is indicative of both excellent performance and acceptance by the test group. Following closely is Dilithium with a rating of approximately 7.6. SPHINCS+ is rated in the middle with a score of approximately 7.0.

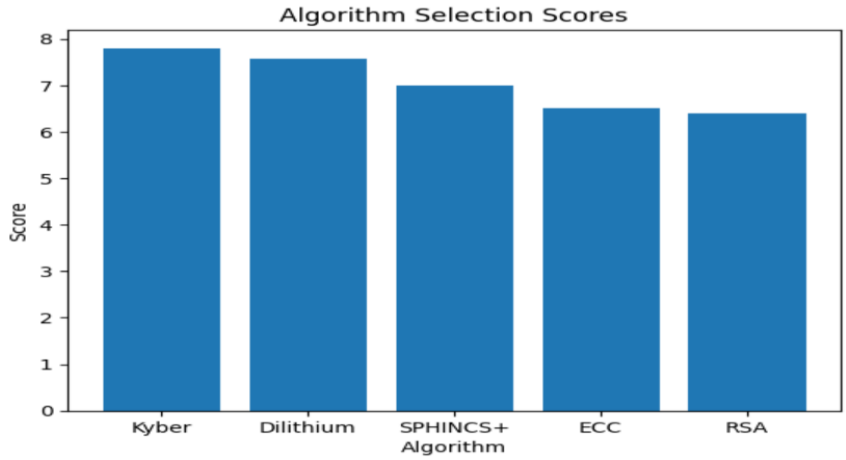


Figure 12: *Algorithm selection scores for different cryptographic techniques.*

The traditional algorithms; however, ECC and RSA have significantly lower score ranges, 6.5 and 6.4 respectively, indicating a lesser degree of effectiveness. The scores indicate a tendency to favor post-quantum algorithms. Such findings reflect an overall trend of moving toward more advanced and future-proof cryptographic systems.

4.6 Evaluation Metrics

Figure 13 shows the Latency performance was measured in three models over several simulation runs. It further shows the classical approach consistently that had the lowest latency value generally between 1 sec to 3 sec with fast execution of performance as measured. The PQC model had more substantial values of Latency that were variable with approximately 3 sec to 9 sec due to an increased degree of computational complexity. The hybrid model provided moderate performance values of Latency in the range of 2 sec to 6 sec providing a good balance between efficiency and performance security. All of the models provided significant variability between runs however their relative positions remain fairly stable. The overall results demonstrate the trade-offs regarding efficiency and security when utilizing either more advanced or greater combined methods of cryptography.

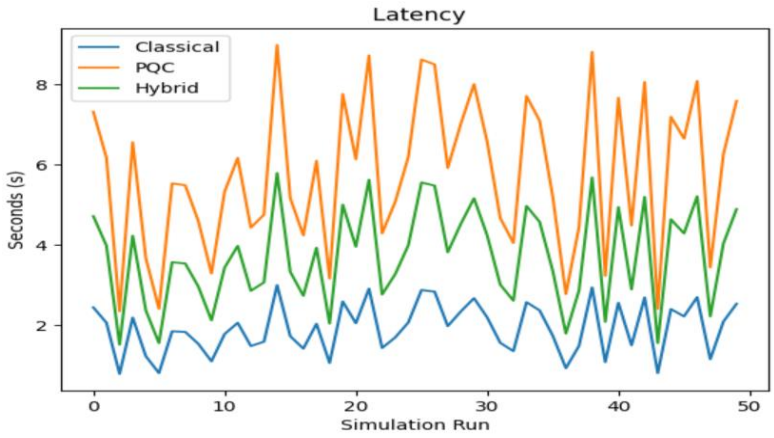


Figure 13: *Latency comparison across classical, PQC, and hybrid models.*

Figure 14 shows the overhead ratios for the three cipher kinds on the different simulations. The classical model presents an overhead ratio equal to 0 (i.e., virtually no additional processing cost); the PQC model shows the greatest overhead ratio (approximately 2.0) as a result of the additional work required to process a post-quantum algorithm; the hybrid model produces an upper-range overhead near 0.9, allowing for a balance between efficient processing speed and high levels of security. All three overhead values exhibit flat trend lines through all runs, indicating no change over time period. Therefore, the figure represents the relationship between overhead and security when implementing advanced cryptographic implementations or combined cryptography implementations.

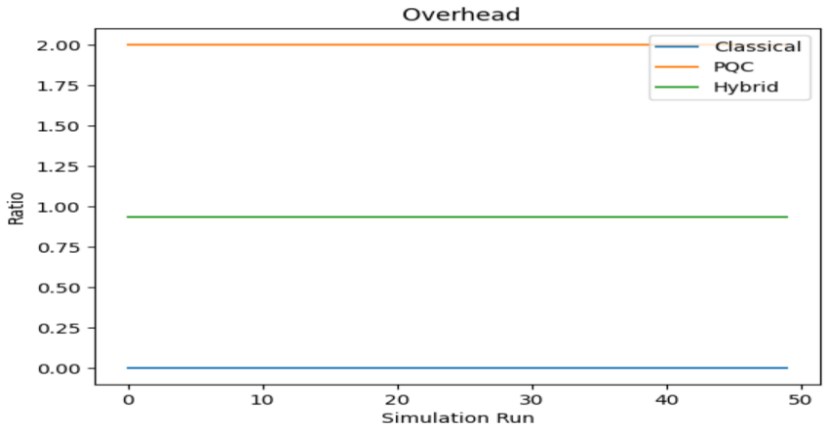


Figure 14: *Overhead comparison across classical, PQC, and hybrid cryptographic models.*

Figure 15 compares the energy consumption of three different cryptographic models through multiple simulation iterations. The classical technique balances maximum energy efficiency, consuming between 2 and 6 units of energy on average. On the other hand the PQC model consumes significantly more energy, fluctuating from an estimated 10 to 36 units due to the higher level of computation complexity required for service protection.

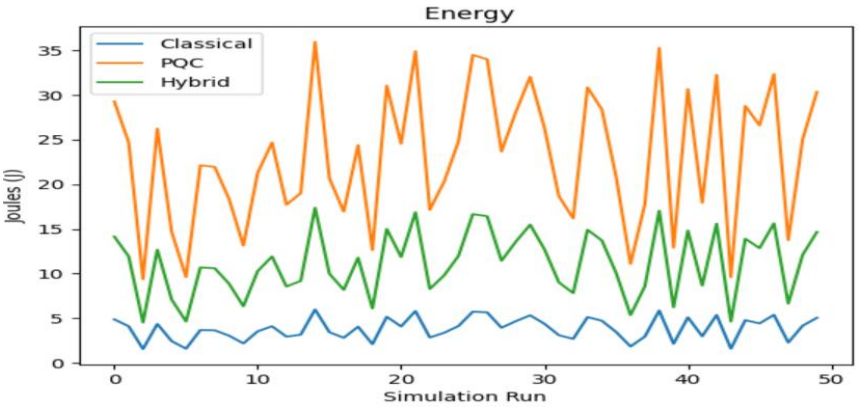


Figure 15: *Energy consumption comparison across classical, PQC, and hybrid cryptographic models.*

The hybrid model is placed in the middle of these extremes in terms of both energy consumption (typically consuming between 5 and 17 units). Although all three models show a significant amount of variability within this dataset, the overall relative energy consumption patterns of these three models are stable. Overall, the figure illustrates the relative trade-off between top-level security and increased energy consumption.

Figure 16 shows the key size variation in the simulation runs for three different cryptographic models. The classical cryptosystems used consistently small key sizes (between 1000 and 2000 bits), requiring less storage and computational resources compared to their post-quantum counterparts. In contrast, the key sizes for the post-quantum models were consistently larger than 4000 bits to approximately 8000 bits in size, indicating stronger security mechanisms. The hybrid models utilized key sizes that were intermediate in size, typically between 2000 and 4000 bits, and thus provided a balance between efficiency and improved security strength. Although key size variations were evident across the simulation runs, the overall relative differences remained constant. Thus, in summary, the results presented in the figures demonstrate the compromises involved with respect to the addition of security strength vs the corresponding incremental increase in key size.

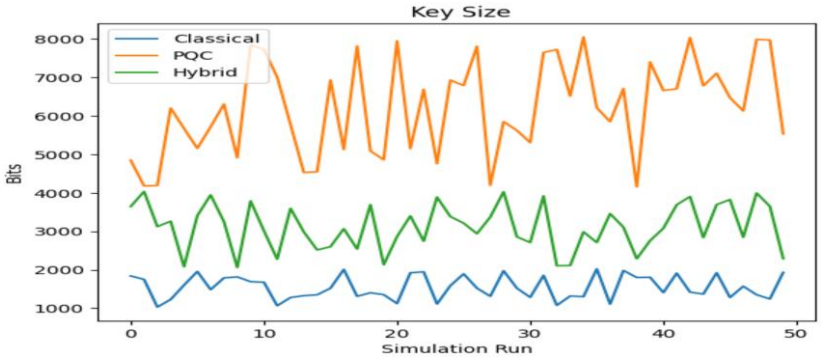


Figure 16: *Key size comparison across classical, PQC, and hybrid cryptographic models.*

Figure 17 shows how well the three types of cryptography work at three different levels (throughput) and based upon multiple simulations. The classical model had the highest throughput of the three models, with very high throughput for most (for example between 90 and 100 megabits per second), showing that it handles data very efficiently. The PQC model had a significantly smaller throughput (70 to about 90 megabits per second on average), mainly due to the additional overhead incurred because of processing an increased amount of computation. The hybrid model performed somewhere in between those two models, typically achieving about 80 to 95 megabits per second, which is both a good balance of throughput and enhanced security compared with classical plus increased security from NR / DSS. While fluctuation in throughput is very evident for each model, the general trend remains consistent with respect to each models throughput performance during the entire simulation length. The figure as a whole illustrates the relationship of trade-offs between better/stronger security systems to be used versus achievable data transfer rates (throughput).

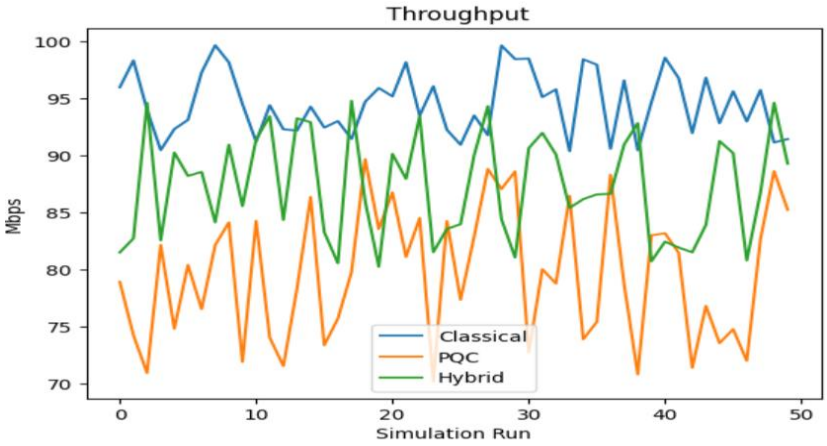


Figure 17: *Throughput comparison across classical, PQC, and hybrid cryptographic models.*

Figure 18 displays the Security level comparisons from three different cryptographic algorithms across a large number of simulated trials. The traditional algorithm consistently received the lowest and most variable security scores ranging from approximately 0.5 to 7, showing comparatively weak and inconsistent protection levels. The other two forms of encryption, PQC and Hybrid, both received consistently higher scores typically between 8 and 10. The Hybrid encryption consistently performed very well with scores that were typically near the maximum range, which indicates greatly improved reliability. While there were some minor variations in scores received on the tests, the overall trend clearly demonstrates how superior the performance of the newer encryption technologies compared to traditional technologies.

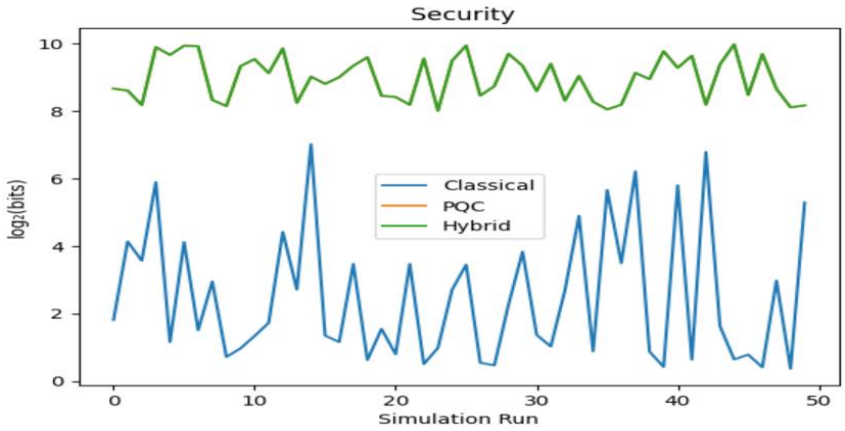


Figure 18: Security level comparison across classical, PQC, and hybrid cryptographic models.

Figure 19 shows the three cryptographic methods of comparison, average performance measures. Further it shows latency, overhead, and key size. This makes classical cryptography efficient, but offers lower security than the others. The PQC (New Post-Quantum) approach shows higher measures than classical with respect to latency, energy usages, and key sizes. PQC has increased levels of security at the expense of performance, compared to classical and hybrid methods.

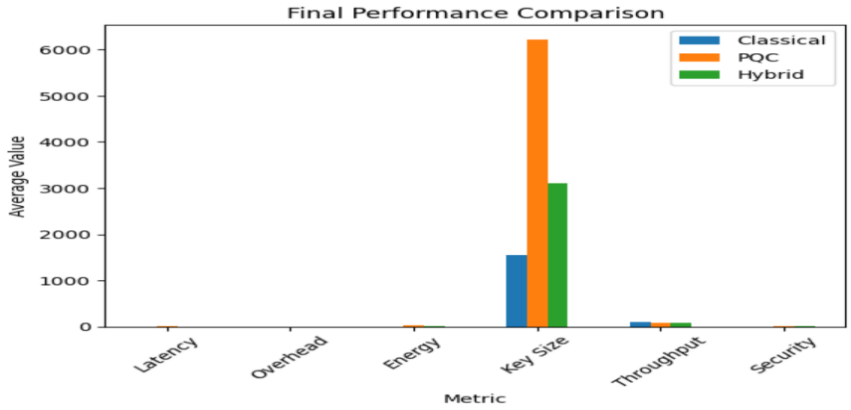


Figure 19: *Final performance comparison across classical, PQC, and hybrid cryptographic models.*

The hybrid combines both extremes, providing moderate levels of latency, energy, and key sizes, while providing for higher throughput and reliable levels of security. Classified and hybrid methods have higher levels of throughput than PQC. Thus the models show trade-offs between efficiency, resource utilization, and strength of security

5. Conclusion

The study emphasizes the slow transition from current traditional forms of crypto to more advanced, quantum resistant forms of crypto that protect critical digital public infrastructure. The results of experiments conducted showed that while Classical models for crypto produce low

latencies, consume little power, and have little overhead, Classical models for crypto are also much weaker than post-quantum models for crypto in terms of security. Conversely, while post-quantum crypto provides good resistance against possible quantum attacks, it has much higher computational complexity, larger keys, and requires much more energy than Classical crypto. A Hybrid crypto model emerges as a relative compromise to provide some of the advantages of Classical models and some of the advantages of post-quantum models. A Hybrid model provides superior security while providing some acceptable level of performance that would support real world deployments. The proposed framework places particular emphasis on the choice of algorithms and sustained monitoring of the security of the infrastructure in order to allow for points of adaptive resistance to new and changing threats, and thus allow a Hybrid/pqc-based framework to be implemented across infrastructures and remain secure from both present threats and future threats.

References

[1] Hasan, Md Asif, Md Tanvir Rahman Mazumder, Md Caleb Motari, Md Shahadat Hossain Shourov, and Md Jahid Howlader. "A Data-Centric Evaluation of AI-Powered Fraud Detection and BI Dashboards in Strengthening Trust and ROI in US E-Commerce." Spanish Journal of Innovation and Integrity 49 (2025): 157-175.

[2] Noor-ul-Ain, W., Muhammad Atta-ur-Rahman, Muhammad Nadeem, and Abdul Ghafoor Abbasi. "Quantum cryptography trends: a milestone in information security." In International Conference on Hybrid Intelligent Systems, pp. 25-39. Cham: Springer International Publishing, 2015.

[3] Krishna, A. Rama, A. S. N. Chakravarthy, and A. S. C. S. Sastry. "A hybrid cryptographic system for secured device to device communication." International Journal of Electrical and Computer Engineering (IJECE) 6, no. 6 (2016): 2962-2970.

[4] Kolade, Titilayo Modupe, Nsidibe Taiwo Aideyan, Seun Michael Oyekunle, Olumide Samuel Ogungbemi, Dooshima Louisa Dapo-Oyewole, and Oluwaseun Oladeji Olaniyi. "Artificial intelligence and information governance: Strengthening global security, through compliance frameworks, and data security." Available at SSRN 5044032 (2024).

[5] Dhinakaran, D., L. Srinivasan, SM Udhaya Sankar, and D. Selvaraj. "Quantum-based privacy-preserving techniques for secure and trustworthy internet of medical things an extensive analysis." Quantum Inf. Comput. 24, no. 3&4 (2024): 227-266.

[6] Althobaiti, Ohood Saud, and Mischa Dohler. "Cybersecurity challenges associated with the internet of things in a post-quantum world." Ieee Access 8 (2020): 157356-157381.

[7] Afshar, Muhammad Zaurez, and Mutahir Hussain Shah. "Leveraging Porter's diamond model: Public sector insights." The Critical Review of Social Sciences Studies 3, no. 2 (2025): 2255-2271.

[8] Nwaga, Philip, and Smart Idima. "Post-quantum cryptographic algorithms for secure communication in decentralized blockchain and cloud infrastructure." International Journal of Computer Applications Technology and Research 11, no. 04 (2022): 155-170.

[9] Jowarder, Rafiul Azim, and Sawgat Jahan. "Quantum computing in cyber security: Emerging threats, mitigation strategies, and future implications for data protection." World Journal of Advanced Engineering Technology and Sciences 13, no. 1 (2024): 330-339.

[10] Shivarudraiah, Arjun. "Quantum Computing's Impact on Banking Encryption: Preparing for Post-Quantum Security." International Journal of AI, BigData, Computational and Management Studies 4, no. 3 (2023): 40-49.

[11] Baseri, Yaser, Vikas Chouhan, and Ali Ghorbani. "Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure." Computers & Security (2026): 104917.

[12] Ahmed, Faraz. "Quantum-resistant cryptography for national security: A policy and implementation roadmap." Int. J. Multidisciplinary on Science and Management 1, no. 4 (2024): 54-65.

[13] Khan, Sadik, P. Krishnamoorthy, Mrinal Goswami, Fayzieva Makhbuba Rakhimjonovna, Salman Arafath Mohammed, and D. Menaga. "Quantum computing and its implications for cybersecurity: A comprehensive review of emerging threats and defenses." Nanotechnology Perceptions 20 (2024): S13.

[14] Fathalla, Efat, and Mohamed Azab. "Beyond classical cryptography: A systematic review of post-quantum hash-based signature schemes, security, and optimizations." IEEE access 12 (2024): 175969-175987.

[15] Majumder, Chinmoy, Arafat Hossain Khan Choain, Md Abu Nasir, and Nasrin Sultana. "Developing Hybrid Post-Quantum Encryption Frameworks for US Databases Integrating Financial, Governmental, and Critical Infrastructure Protections." Journal of International Accounting and Financial Management 3, no. 1 (2026): 1-18.

[16] Shirisha, N., H. M. Manoj, Shaik Jakeer Hussain, Rajitha Kotoju, Ramakrishna Kolikipogu, and A. Mohan. "Post-quantum security framework for resource-constrained systems: emerging trends, challenges, sustainability, and future directions." Discover Computing 29, no. 1 (2026): 85.

[17] Devaraj, Poojitha, Syed Abrar Chaman Basha, Nithesh Nair Panarkuzhiyil Santhosh, and Niharika Panda. "A Post-Quantum Secure Architecture for 6G-Enabled Smart Hospitals: A Multi-Layered Cryptographic Framework." Future Internet 18, no. 3 (2026): 165.

[18] Jamolova, Gulbanbegim, Maloxat Axmedova, Feruzaxon Odilova, Feruza Urinboyeva, Sadokatxon Yuldasheva, Polat Shokirov, and Kamolbek Masharipov. "Quantum Safe Cryptographic Frameworks for Securing National Digital Currencies and Economic Infrastructure." Journal of Internet Services and Information Security (JISIS) 16, no. 1 (2026): 237-252.

[19] Olisa, Anthony Obulor, Michael Olayinka Gbadebo, Nanyeneke Ravana Mayeke, Tunbosun Oyewale, and Faith Hauwa Oluwapamilerin Kolo Oladoyinbo. "Quantum-Resistant Cryptographic Protocols for CBDC Interoperability: A Cross-Border Settlement Security Framework." (2026).

[20] Faval, Ricardo Alves, Rodrigo Moreira, and Flávio de Oliveira Silva. "Empowering Mobile Networks Security Resilience by using Post-Quantum Cryptography." arXiv preprint arXiv:2603.28626 (2026).

[21] Kannan, Prabakaran. "Post-Quantum Cryptography for Resource-Constrained IoT and Edge Devices: A No-Std Rust Implementation Framework."

[22] Rassekhnia, Jonatan. "QERS: Quantum Encryption Resilience Score for Post-Quantum Cryptography in Computer, IoT, and IIoT Systems." arXiv preprint arXiv:2601.13399 (2026).

[23] Khan, Abdullah Ayub, Asif Ali Laghari, Hamad Almansour, Leila Jamel, Fahima Hajjej, Vania V. Estrela, Mohamad Afendee Mohamed, and Sajid Ullah. "Quantum computing empowering blockchain technology with post quantum resistant cryptography for multimedia data privacy preservation in cloud-enabled public auditing platforms." Journal of Cloud Computing 14, no. 1 (2025): 43.

[24] Balogun, Adebayo Yusuf. "Post-quantum cryptography and encryption standards: safeguarding patient data against emerging cyber threats in telemedicine." Asian Journal of Research in Computer Science 18, no. 3 (2025): 345-367.

[25] Reddy, Nalavala Ramanjaneya, Supriya Suryadevara, K. Guru Raghavendra Reddy, Ramisetty Umamaheswari, Ramakrishna Guttula, and Rajitha Kotoju. "Quantum secured blockchain framework for enhancing post quantum data security." Scientific Reports 15, no. 1 (2025): 31048.

[26] Meenalochini, P. "Implementation of Quantum-Resistant Key Exchange Protocols in IoT Networks for Safeguarding Critical Infrastructure Against Post-Quantum Cyber Threats."

[27] de Haro Moraes, Daniel, João Paulo Aragão Pereira, Bruno Estolano Grossi, Gustavo Mirapalheta, George Marcel Monteiro Arcuri Smetana, Wesley Rodrigues, Courtnay Nery Guimarães Jr, Bruno Domingues, Fábio Saito, and Marcos Simplício. "Applying post-quantum cryptography algorithms to a dlt-based cbdc infrastructure: Comparative and feasibility analysis." Cryptology ePrint Archive (2024).

[28] Scalise, Paul, Robert Garcia, Matthew Boeding, Michael Hempel, and Hamid Sharif. "An applied analysis of securing 5g/6g core networks with post-quantum key encapsulation methods." Electronics 13, no. 21 (2024): 4258.

[29] Romanenkov, Aleksandr Mikhailovich. "Digital public administration infrastructure and its effectiveness." Personality Society 2, no. 3 (2021): 4-10.

[30] Serrano, Will. "Digital systems in smart city and infrastructure: Digital as a service." Smart cities 1, no. 1 (2018): 134-154.

[31] Brucherseifer, Eva, Hanno Winter, Andrea Mentges, Max Mühlhäuser, and Martin Hellmann. "Digital Twin conceptual framework for improving critical infrastructure resilience." at-Automatisierungstechnik 69, no. 12 (2021): 1062-1080.

[32] Alhamarneh, Raed Ahmed, and Manmeet Mahinderjit Singh. "Strengthening internet of things security: Surveying physical unclonable functions for authentication, communication protocols, challenges, and applications." Applied Sciences 14, no. 5 (2024): 1700.