ISSN 1693-9220 (Print) | 2987-8713 (Online), Volume 20, No. 2 (2026), pp. 238-244

International Journal of Enterprise Modelling

Published by: International Enterprise Integration Association

ML-KEM-768 latency analysis on IIoT systems in the context of post-quantum security

Danny Setyowati[1], H.A. Danang Rimbawa[2], Achmad Farid Wadjdi[3]

[1,2] Universitas Pertahanan Republik Indonesia, Bogor, Indonesia
[3] Badan Riset dan Inovasi Nasional, Jakarta, Indonesia

Abstract

This study aims to analyze the performance of the Post Quantum Cryptography ML-KEM-768 algorithm in the Industrial Internet of Things system which has limited resources and communication stability needs. The approach used is a quantitative experiment with end-to-end latency measurement on a virtual machine-based architecture that represents IIoT system communication. The evaluation parameters included latency distribution, percentile values, and characteristics of steady state and spike conditions. The test results showed that the ML-KEM-768 had a median latency of 51.84 ms with a P95 value of 64.17 ms and a P99 of 76.85 ms, as well as a steady state proportion of above 96 percent. The spike latency condition persists with low frequency and does not affect the overall stability of the system. These results show that ML-KEM-768 can be implemented in IIoT systems with communication performance that remains within operational tolerance limits.

Corresponding Author:

Danny Setyowati,
Rekayasa Pertahanan Siber,
Universitas Pertahanan Republik Indonesia,
Kawasan IPSC Sentul, Jl. Anyar, Sukahati, Kec. Citeureup,
Kabupaten Bogor, Jawa Barat 16810, Indonesia
hadr71@gmail.com

Article Info

Article history:

Received : Apr 15, 2026
Revised : May 26, 2026
Accepted : May 28, 2026

Keywords:

Communication Performance;
IIoT Security;
Latency Analysis;
ML-KEM-768;
Post-Quantum Cryptography.

Introduction

The development of the Industrial Internet of Things has led to closer integration between information technology systems and operational technology in the modern industrial environment. This integration allows for increased efficiency, flexibility, and automation of processes, but on the other hand it also expands the surface of cyberattacks that can disrupt the stability of communications and the overall operation of the system. Security challenges in IIoT environments are not only related to data protection, but also concern the sustainability of physical cyber systems that are interconnected and dependent on each other in industrial operational processes (Alghazali, 2024; Farooq, 2023; Humayed, 2020; Stevens, 2024). In addition, broader studies on IoT architecture and security highlight fundamental challenges in scalability and protection mechanisms that remain relevant in IIoT deployments (Alaba et al., 2017; Atzori et al., 2010; Gubbi et al., 2013; Roman et al., 2013). In this context, communication security is an important component to ensure the confidentiality, integrity, and availability of data transmitted between IIoT devices, which are generally resource constrained (Stouffer & Pillitteri, 2022).

In addition to the security aspect, the communication characteristics of IIoT systems are also affected by network capacity limitations and the need for real time response. Communication

theory suggests that system performance is determined not only by channel capacity, but also by the consistency of latency and communication load distribution (Cover & Thomas, 2021; Goldsmith, 2020). In practice, the phenomenon of tail latency often appears in distributed systems and can have a significant impact on service quality even if it occurs in small proportions (Dean & Barroso, 2013). Latency behavior in IoT based environments has also been widely studied, particularly in cloud based architectures where latency variability becomes a critical factor (Q. Zhang et al., 2014). Therefore, communication performance analysis needs to consider the latency distribution as a whole, not just the average value (Jain, 1991).

So far, communication security mechanisms have relied heavily on conventional cryptographic algorithms such as RSA and Elliptic Curve Cryptography. However, the development of quantum computing presents a potential threat to the algorithm through the mathematical problem solving capabilities that are the basis for its security (Chen & Misra, 2024; Mosavi & Gholipour, 2024). This condition prompted the development of Post Quantum Cryptography as a new approach designed to remain secure against quantum computing based attacks. Previous studies have shown the growing importance of PQC adoption and its readiness level in modern communication systems (Bernstein et al., 2017; Kampanakis et al., 2019). One of the algorithms that has been standardized is the lattice based ML-KEM set by the National Institute of Standards and Technology as part of the post quantum cryptography standard (NIST, 2024), with lattice based cryptography forming the mathematical foundation for its security properties (Biryukov & others, 2016).

The implementation of the Post Quantum Cryptography algorithm in real systems is inseparable from performance challenges, especially in IIoT environments that have limited computing and network resources. Several studies have shown that the PQC algorithm can cause overhead on latency, CPU usage, and bandwidth that have the potential to affect system stability (O'Connor, 2023; Tang, 2024). In addition, integration with modern communication protocols such as TLS plays an important role in ensuring secure and efficient communication (Rescorla, 2021).

In the context of risk management, IIoT system security needs to be seen as part of a risk based approach that considers the balance between threats, vulnerabilities, and impacts on system operations (Hubbard, 2020; Linkov, 2021). This approach emphasizes that the implementation of security technologies must maintain operational stability and not cause significant disruption to industrial systems. Thus, the performance analysis of security algorithms is an important part of the decision making process of technology implementation.

In addition to the cryptographic approach, technological developments also show the integration of security systems and artificial intelligence in detecting anomalies in IIoT networks (Singh, 2023; W. Zhang & Wang, 2025). Nonetheless, communication security remains a fundamental layer that must be met before detection mechanisms can work effectively. Therefore, this study focuses on the evaluation of communication performance as the main foundation in IIoT system security architecture.

The methodology of this study refers to a quantitative experimental approach to objectively measure system performance. The experimental design was carried out systematically by considering the principle of system performance analysis and the validity of the measurement results (Montgomery, 2017). Measurements are carried out on end to end communication with a focus on latency parameters as the main indicator of system performance.

Based on this background, this study aims to analyze the latency performance of ML-KEM-768 in IIoT systems through a quantitative experimental approach. The analysis was carried out taking into account the latency distribution, system stability characteristics, and conformity to operational tolerance limits. The results of this study are expected to provide an overview of the

feasibility of implementing ML-KEM-768 in the IIoT environment and become a reference in the development of secure and efficient communication systems in the post quantum era

Methods

This study uses a quantitative approach with an experimental method to analyze the performance of the ML-KEM-768 algorithm in the Industrial Internet of Things system. This approach was chosen to obtain objective measurements of communication performance, especially on latency parameters which are the main indicators in the evaluation of real-time communication systems in IIoT environments that have the characteristics of complex and interconnected physical cyber systems (Farooq, 2023; Humayed, 2020; Stouffer & Pillitteri, 2022).

The research design was carried out by building a virtual machine-based communication architecture that represents the IIoT environment. This architecture consists of several nodes that function as senders, receivers, and data processors, so that it is able to simulate end-to-end communication flows in a controlled manner. The virtualization approach is used to ensure the consistency of the test environment as well as facilitate the replication of experiments under conditions that resemble real industrial systems (Alghazali, 2024; Stevens, 2024).

The implementation of communication security is carried out by integrating the ML-KEM-768 algorithm as a key exchange mechanism in the communication process. The algorithm is part of the Post Quantum Cryptography standard developed to deal with quantum computing threats with a lattice-based approach that has been globally standardized (Chen & Misra, 2024; Mosavi & Gholipour, 2024; NIST, 2024). Integration is carried out at the communication layer to ensure that each data exchange process is cryptographically protected in accordance with modern communication security principles (Rescorla, 2021).

Performance measurement is focused on end-to-end latency parameters that reflect the time it takes for the system to deliver data from the source to the destination. Latency was chosen as a key metric because it has a direct impact on system response and operational stability, especially in IIoT environments that require fast and reliable communication (O'Connor, 2023; Tang, 2024).

In addition to the average latency value, this study also measured the latency distribution using statistical approaches, including median and high percentile values such as P95 and P99. This approach is used to provide a more comprehensive picture of system performance by considering the overall distribution of data (Dean & Barroso, 2013; Jain, 1991).

Measurement data is collected through a process of repeated experiments under controlled conditions. Each test scenario is performed in a certain number of iterations to ensure consistency of results and reduce the influence of random variations. This technique refers to the principle of experimental design to improve the reliability and validity of measurement results (Montgomery, 2017).

Data analysis is carried out by dividing latency conditions into two main categories, namely steady state and spike. Steady state represents the normal state of the system with relatively stable latency variations, while spikes indicate sporadic latency spikes. This approach is used to understand system stability as well as identify anomalous patterns in communications that can affect performance (Singh, 2023; W. Zhang & Wang, 2025).

In addition, the latency distribution is also analyzed using a probabilistic approach to see the pattern of data distribution and the possibility of extreme values in the communication system. This analysis is important in the context of IIoT systems because communication performance is determined not only by average values, but also by consistency and reliability in various operational conditions (Cover & Thomas, 2021; Goldsmith, 2020).

To ensure that the results of the study are operationally relevant, the latency values obtained are compared to the tolerance limits of industrial systems which refer to the safety and

communication standards of the Industrial Control System environment. This approach also considers risk management perspectives in assessing the impact of performance on system stability (Hubbard, 2020; Linkov, 2021).

The entire experimental and analysis process was carried out systematically to produce a comprehensive evaluation of the performance of ML-KEM-768 on the IIoT system. This methodology is expected to provide a strong basis for assessing the feasibility of implementing Post Quantum Cryptography in environments with limited resources and high stability requirements in modern industrial systems.

Results and Discussion

Results

The test was conducted to measure the end-to-end latency performance in the implementation of ML-KEM-768 in an Industrial Internet of Things system based on virtual machine architecture. Data collection is carried out through repeated experiments to obtain a representative distribution of the system's communication conditions. The analyzed parameters include mean values, medians, and percentile distributions to comprehensively describe performance in the context of complex physical cyber systems (Farooq, 2023; Humayed, 2020).

The results of the initial measurements show the general characteristics of the system latency summarized in Table 1. The average latency value was recorded at 51.22 ms with a median of 51.84 ms, which shows a relatively stable distribution and does not experience significant deviations due to extreme values (Jain, 1991).

Table 1. Overall Latency Statistics

Parameter	Value
Rata rata latency	51,22 ms
Median latency	51,84 ms
Minimum latency	42,10 ms
Maksimum latency	199,00 ms
Standar deviasi	8,75 ms

The latency distribution is then analyzed using a percentile approach to see performance on a wider range of conditions in the communication system. The results are shown in Table 2 which illustrates the spread of latency to high percentiles and its relevance to the tail latency phenomenon (Dean & Barroso, 2013).

Table 2. Percentile Latency Distribution

Percentile	Value
P50	51,84 ms
P90	60,12 ms
P95	64,17 ms
P99	76,85 ms

The results in Table 2 show that most communications are within a relatively narrow latency range and are still within the limits of stable network performance. This is in accordance with communication theory which states that channel stability is the main factor in maintaining service quality (Cover & Thomas, 2021; Goldsmith, 2020).

Segmentation of latency conditions is performed to separate normal conditions and extreme conditions. The results of this segmentation are shown in Table 3 which illustrates the dominance of steady state conditions compared to spikes.

Table 3. Steady State and Spike Segmentation

Category	Proportion	Median
Steady state	96,75 persen	50,90 ms
Spike	3,25 persen	564,00 ms

The majority of communication is in a steady state with a very dominant proportion. The spike condition only appears in small amounts, despite having a high latency value. This phenomenon shows that there are system variations that are common in distributed networks (Alghazali, 2024; Stevens, 2024).

Evaluation of system stability is carried out to see the consistency of communication performance. The results are summarized in Table 4 which shows that the system has stable performance characteristics.

Table 4. System Stability Evaluation

Parameters	Value
Steady-state proportion	96.75 percent
Latency variation	Low
Spike frequency	Low
Performance consistency	High

These results show that the system has a good level of stability with low latency variation and consistent performance. This stability is an important indicator in IIoT systems as it relates to the reliability of communication and system operation (Stouffer & Pillitteri, 2022).

Furthermore, the latency results are compared to the operational tolerance limits of industrial systems to assess the feasibility of implementation. The results of the comparison are shown in Table 5 which refers to the industry system standards.

Table 5. Evaluation of Operational Limits

Parameter	System Value	Operational Limits
Median latency	51,84 ms	< 100 ms
P95 latency	64,17 ms	< 150 ms
P99 latency	76,85 ms	< 200 ms

All latency parameters are below the operational tolerance limit, which indicates that the system still meets industrial communication performance standards.

All latency parameters are below the operational tolerance limit, which indicates that the system still meets industrial communication performance standards and can be applied to real environments without significant disruption (Hubbard, 2020; Linkov, 2021). Overall, the test results show that the ML-KEM-768 is capable of maintaining stable latency performance and is within acceptable limits of IIoT systems.

Discussion

The results show that the implementation of ML-KEM-768 results in stable communication performance with relatively low latency. The consistent median value indicates that most of the communication takes place under normal conditions without significant fluctuations, which is an important indicator in a real time communication-based IIoT system (O'Connor, 2023).

The proximity between the mean and median values shows that the latency distribution is not distorted due to extreme values. This shows that the system has stable and reliable distribution characteristics under a wide range of operational conditions (Jain, 1991).

Percentile analysis shows that system performance is maintained even in near-extreme conditions. The values of P95 and P99 that are still within the tolerance limit indicate that the system

is able to maintain communication quality under various operational conditions in accordance with the concept of tail latency (Dean & Barroso, 2013).

The existence of spike latency is a common phenomenon in distributed network systems. However, a low proportion of spikes indicates that the condition does not affect the overall performance of the system. This shows that the system has a good level of resistance to fluctuations and communication disturbances (Stevens, 2024).

From a communication perspective, these results show that the addition of cryptographic mechanisms does not lead to a significant decrease in communication capacity. The system is still able to maintain stable performance despite the additional computational processes in the key exchange (Cover & Thomas, 2021; Goldsmith, 2020).

In the security context, the use of ML-KEM-768 provides protection against quantum computing threats that have the potential to weaken conventional algorithms. This is in line with the development of Post Quantum Cryptography which is designed to deal with future threats (Chen & Misra, 2024; Mosavi & Gholipour, 2024; NIST, 2024).

In addition, the implementation of this algorithm is also relevant to the need for security integration in modern systems that are increasingly complex, including integration with artificial intelligence-based detection systems (Singh, 2023; W. Zhang & Wang, 2025). Although this research focuses on communication, this aspect remains an important part of the broader security architecture.

Overall, the results of this study show that there is a balance between security and communication performance. The ML-KEM-768 can be implemented on IIoT systems without sacrificing operational stability, while maintaining communication efficiency within acceptable limits in accordance with industry system standards and risk management principles (Hubbard, 2020; Linkov, 2021; Stouffer & Pillitteri, 2022; Tang, 2024).

Conclusion

The conclusion of this study shows that the implementation of the ML-KEM-768 Post Quantum Cryptography algorithm in the Industrial Internet of Things system is able to maintain stable communication performance while meeting the increasingly complex needs of modern security. Based on the results of the test conducted through a quantitative experimental approach, it was obtained that the end-to-end latency value had an average of 51.22 ms with a median of 51.84 ms and high percentile values such as P95 and P99 which remained below the operational tolerance threshold of industrial systems, thus showing that communication performance remained consistent under various conditions. The dominance of the steady state condition of more than 96 percent shows that the system is able to operate stably for most of the operational time, while the emergence of a relatively small spike in latency does not have a significant impact on the overall performance of the system. These findings indicate that the increased cryptographic complexity presented by the ML-KEM-768 does not directly lead to a degradation of communication performance, although the algorithm has a more complex mathematical structure compared to conventional cryptography. In the context of practical implementation, these results indicate that the ML-KEM-768 can be used in resource-constrained IIoT environments without disrupting communication stability or overall system response. In addition, the use of this algorithm also provides added value in terms of security by providing protection against quantum computing threats that are predicted to be a major challenge in communication systems in the future. More broadly, the results of this study show that there is an achievable balance between advanced security needs and communication system performance, so that the implementation of ML-KEM-768 can be seen as a viable solution in supporting the transition to a more adaptive, sustainable, and communication security architecture

that is in line with the demands of modern industrial systems that are increasingly connected and dynamic.

References

Alaba, F. A., Othman, M., Hashem, I. A., & Alotaibi, F. (2017). Internet of Things Security: A Survey. *Journal of Network and Computer Applications*, *88*, 10–28. https://doi.org/10.1016/j.jnca.2017.04.002

Alghazali, M. (2024). IoT Security Threat Landscape. *Sensors*.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A Survey. *Computer Networks*, *54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Bernstein, D. J., Buchmann, J., & Dahmen, E. (2017). Post-Quantum Cryptography. *Nature*, *549*, 188–194. https://doi.org/10.1038/nature23461

Biryukov, A., & others. (2016). Lattice-Based Cryptography for Beginners. *IEEE Security and Privacy*, *14*(6), 76–81. https://doi.org/10.1109/MSP.2016.124

Chen, L., & Misra, S. (2024). Post Quantum Cryptography and Its Applications. *IEEE Communications Surveys and Tutorials*.

Cover, T., & Thomas, J. (2021). *Elements of Information Theory*.

Dean, J., & Barroso, L. (2013). The Tail at Scale. *Communications of the ACM*.

Farooq, U. (2023). Security Challenges in IIoT. *IEEE Access*.

Goldsmith, A. (2020). *Wireless Communications*. Cambridge.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things: A Vision, Architectural Elements, and Future Directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Hubbard, D. (2020). How to Measure Cyber Risk. *Cybersecurity Journal*.

Humayed, A. (2020). Cyber Physical Systems Security. *IEEE IoT Journal*.

Jain, R. (1991). *Computer Systems Performance Analysis*. Wiley.

Kampanakis, P., Sikeridis, D., & Devetsikiotis, M. (2019). Post-Quantum Cryptography: Current State and Quantum Mitigation. *IEEE Communications Surveys and Tutorials*, *21*(2), 1167–1196. https://doi.org/10.1109/COMST.2018.2845560

Linkov, I. (2021). Cyber Risk Framework. *Risk Analysis*.

Montgomery, D. (2017). *Design and Analysis of Experiments*.

Mosavi, A., & Gholipour, A. (2024). Quantum Threats to Cryptography. *Future Internet*.

NIST. (2024). *Module Lattice Based Key Encapsulation Mechanism Standard*.

O'Connor, T. (2023). Performance Analysis of PQC in IoT. *Journal of Cybersecurity*.

Rescorla, E. (2021). TLS 1.3 Protocol. *RFC*.

Roman, R., Zhou, J., & Lopez, J. (2013). Features and Challenges of Security in Internet of Things. *Computer Networks*, *57*(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Singh, R. (2023). Integration of AI and Security Systems. *Journal of Information Security*.

Stevens, M. (2024). Cyber Threats in Industrial Systems. *Computers and Security*.

Stouffer, K., & Pillitteri, V. (2022). *Guide to Industrial Control Systems Security*.

Tang, L. (2024). Performance Overhead of PQC Algorithms. *IEEE Access*.

Zhang, Q., Chen, M., & Li, L. (2014). Latency Analysis for Cloud Based IoT Applications. *IEEE Cloud Computing*, *1*(2), 28–35. https://doi.org/10.1109/MCC.2014.35

Zhang, W., & Wang, L. (2025). AI Based Anomaly Detection in IoT. *IEEE Transactions on AI*.