National Research Journal of Information Technology & Information Science
Volume No: 13, Issue No: 1, Year: 2026 (January-June)
PP: 264-272
ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

PERFORMANCE ANALYSIS OF POST-QUANTUM CRYPTOGRAPHY IN TLS-SECURED LOW-POWER IOT SYSTEMS

Gurwinder Singh

Department of Computer Science and Applications
Sikh National College, Banga, India

ABSTRACT

Advancements in quantum computing are posing a serious threat to the security of commonly used public-key cryptographic systems, and consequently, to the safety of digital communications that depend on them. In response to this emerging risk, the US National Institute of Standards and Technology (NIST) has been actively working on identifying and standardizing post-quantum cryptographic algorithms that can withstand attacks from quantum machines.

At the same time, ensuring security in low-power IoT devices remains a major challenge. Even with traditional cryptographic methods, these devices struggle due to limited energy availability, constrained processing capabilities, and restricted memory resources. This study, presents a comprehensive analysis of how candidate post-quantum key encapsulation mechanisms (KEMs) and digital signature algorithms (DSAs), proposed through the NIST standardization process, perform within a modern TLS-based IoT environment.

To explore this, selected KEMs and DSAs were implemented in a representative low-power IoT infrastructure, and their performance was evaluated on an edge device. The analysis focused on key factors such as energy consumption, communication latency, and memory usage during TLS handshakes.

The results provide several important insights. First, the increased latency observed in TLS handshakes is primarily caused by the larger data sizes associated with post-quantum algorithms, rather than the computational complexity of the cryptographic operations themselves. Second, combining multiple digital signature schemes strategically can improve overall efficiency in terms of energy, latency, and memory—challenging NIST's current approach of standardizing a single algorithm. Finally, the study demonstrates that various classes of post-quantum algorithms, including code-based, isogeny-based, and lattice-based methods, can be effectively deployed on resource-constrained IoT devices such as those powered by Cortex-M4 microcontrollers, without significantly compromising battery life. This finding contrasts with the common assumption that specialized hardware acceleration is essential for practical implementation.

Keywords: Post-quantum cryptography; energy-efficient secure IoT systems; TLS-based security; key encapsulation mechanisms; digital signature schemes.

1. INTRODUCTION

The Internet of Things (IoT) is rapidly transforming many aspects of everyday life. From improving comfort in smart homes to supporting healthcare systems and optimizing industrial operations in the Industrial IoT (IIoT), the adoption of IoT devices is expanding at an unprecedented pace.

Despite these benefits, IoT ecosystems introduce significant security challenges. As the number of connected devices increases, so does the scale and sophistication of cyberattacks targeting them. This growing threat landscape makes security one of the most pressing

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

concerns in IoT deployments. A recent example is the vulnerability discovered in the widely used Log4j library, which highlighted how a single weakness in commonly used software can have far-reaching consequences across multiple industries.

Adding to these concerns, the rapid progress in quantum computing is emerging as a new risk factor. Advances in this field have the potential to undermine the security of existing cryptographic mechanisms embedded in many software systems, raising serious questions about the future resilience of current information security practices.

Secure communication plays a vital role in Industrial IoT (IIoT) environments, as the data transmitted over networks often includes sensitive operational details, critical infrastructure information, and proprietary industrial knowledge[1]. To protect this data, most systems rely on cryptographic protocols such as Transport Layer Security (TLS), which combine symmetric encryption with public key cryptography (PKC). While these cryptographic techniques are considered secure against classical computing attacks, their underlying mathematical foundations could be efficiently solved using quantum computing algorithms, a concept introduced nearly three decades ago. Although such powerful quantum machines were not available at that time, current advancements suggest that practically relevant quantum computers may emerge within this decade[2,3].

Recognizing this potential threat, the US National Institute of Standards and Technology (NIST) initiated a standardization effort focused on post-quantum cryptography (PQC). The goal is to identify and standardize new public key algorithms, including key encapsulation mechanisms (KEMs) and digital signature algorithms (DSAs), that can resist quantum-based attacks. These candidate algorithms are evaluated not only for their security strength but also for their performance characteristics. This makes it crucial to study how factors like computational cost and communication overhead impact their deployment in real-world scenarios, particularly in constrained environments such as low-power IoT systems. It is equally important to determine whether existing IoT hardware platforms can handle these new algorithms within strict energy and resource limits, or if specialized hardware acceleration will be necessary[4-7].

A comprehensive evaluation of PQC requires considering the entire system, including all layers of the communication protocol stack. While earlier studies have explored the use of certain post-quantum KEMs on low-power IoT devices, these analyses were limited in scope, as they did not include all relevant algorithms or account for recent updates. Moreover, they did not incorporate post-quantum digital signatures or public key infrastructures (PKIs), leaving systems vulnerable to quantum-enabled man-in-the-middle attacks[8].

To address these limitations, this work presents a detailed investigation of the transition from conventional cryptography to PQC within a realistic low-power IoT framework. The system under study integrates technologies such as Bluetooth Low Energy (BLE), IPv6 over low-power wireless personal area networks (6LoWPAN), Transmission Control Protocol (TCP), TLS, and the Message Queuing Telemetry Transport (MQTT) protocol.

On the device side, post-quantum capabilities were implemented on a resource-constrained IoT edge device by extending the mbedTLS library, enabling seamless integration of PQC into the TLS 1.2 handshake process. On the server side, the OQS-OpenSSL library was updated to include the latest versions of Round 3 KEMs, along with added support for post-quantum digital signatures and certificates. The study evaluates key performance metrics such as latency, energy consumption, and memory usage during PQC-enabled TLS handshakes, and compares them with traditional elliptic curve-based approaches.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

Given the ongoing standardization efforts, NIST has emphasized the need for more empirical performance data on the integration of PQC into internet protocols, highlighting the importance of studies like this in guiding future adoption.

2. LITERATURE REVIEW

This work brings together post-quantum cryptography for use in both servers and embedded devices, along with its deployment in current communication protocols and energy-efficient secure IoT systems. Since these domains are still actively evolving, only a limited amount of closely related research is currently available.

On the server side, the Open Quantum Safe (OQS) initiative is a key effort aimed at making it easier to prototype post-quantum cryptographic (PQC) algorithms on conventional computers and servers[9]. As part of this project, PQC schemes have been incorporated into OpenSSL implementations for TLS 1.2 and TLS 1.3.

In a related study, a network emulation setup was created using OQS-based implementations to analyze the strengths and limitations of applying PQC within TLS. The findings indicated that in high-speed, stable networks, the TLS handshake duration is largely influenced by public-key cryptographic computations. However, in environments with higher packet loss, network communication overhead becomes the dominant factor affecting overall handshake time[10].

On the client side[11], the pqm4 project has developed a library that provides assembler-optimized implementations of most post-quantum cryptographic primitives for ARM Cortex-M4 processors, which are also used in this study. Benchmarking carried out by Kannwischer and colleagues demonstrated that these optimizations lead to substantial performance improvements across many of the cryptographic primitives.

Further research using the same library also evaluated energy consumption, revealing that certain lattice-based algorithms exhibit some of the lowest energy requirements among all candidates proposed in the NIST standardization process[12].

A complete post-quantum TLS implementation for embedded systems was proposed in [13]. In this work, the researchers incorporated a single parameter set of the PQC key encapsulation mechanism KYBER along with the digital signature algorithm SPHINCS+ into the mbedTLS library. They then evaluated its performance on three different hardware platforms, with each device functioning either as a client or a server. The results indicated that TLS handshakes using these two cryptographic schemes are practically achievable on the tested devices. However, the study did not account for communication overhead in its evaluation and considered only one KEM and one DSA, without reporting energy consumption metrics.

An initial analysis of certain post-quantum KEMs for resource-constrained IoT devices was conducted, showing that specialized hardware accelerators are not strictly necessary to achieve efficient implementations. Nevertheless, that study did not cover all NIST Round 3 KEM candidates, and it remains unclear whether similar conclusions apply to post-quantum digital signature algorithms as well.

So far, existing studies have mainly concentrated on cryptographic operations executed on embedded platforms or on evaluations carried out in conventional desktop environments. To the best of knowledge, there is still no comprehensive system-level analysis that examines the performance of post-quantum digital signature algorithms (DSAs) and key encapsulation mechanisms (KEMs) within a realistic low-power IoT application. This gap is somewhat

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

unexpected, especially given the extensive research on energy-efficient hardware accelerators for PQC algorithms, where several works suggest that such accelerators are essential for enabling PQC on resource-constrained devices.

This paper addresses this limitation by providing a detailed evaluation of post-quantum DSAs and KEMs in a low-power IoT context. The study also aligns with NIST's recommendations for obtaining more empirical performance data of PQC algorithms in real protocol-based scenarios.

3. POST- QUANTUM SAFE IOT INFRASTRUCTURE

This section presents the IoT infrastructure adopted in this study, which serves as a test environment for evaluating the post-quantum cryptographic candidates under consideration by the US NIST for standardization. In addition, suitable public key infrastructures (PKIs) designed for this setup are outlined and specify the key encapsulation mechanisms (KEMs) and digital signature algorithms (DSAs) that were included in the analysis[14].

3.1 Experimental Setup

The IoT infrastructure considered in this work comprises three main components: edge devices (sensors or acuators), a gateway, and a cloud-based server. For evaluation, a secure, low-power IoT setup was implemented. The edge devices are based on the Nordic Semiconductor nRF52840 system-on-chip, which uses an ARM Cortex-M4 microcontroller. This platform was selected because it is also used by NIST as a reference hardware for post-quantum cryptography evaluations. It is well-suited for energy-constrained IoT environments and includes features such as the ARM CryptoCell-310 security module, Bluetooth 5 support, 1 MB flash memory, and 256 KB RAM. The CryptoCell provides hardware acceleration for cryptographic operations like ECDSA, ECDHE, AES-128, and SHA-2. Standard TLS over TCP and IPv6 is used to ensure end-to-end security between the device and the server, rather than lightweight alternatives like DTLS.

On the backend, a Linux-based server equipped with an Intel Xeon Silver 4214 processor and MQTT broker is used. The processor supports AVX instructions, which are commonly leveraged in optimized post-quantum cryptographic implementations, making it suitable for this study. A Raspberry Pi 3 serves as the gateway, functioning purely as a transparent bridge between BLE and Ethernet without interfering with TLS processing. A BLE connection interval of 20 ms is configured to balance responsiveness, throughput, and energy efficiency. Although TLS 1.3 is the latest version, TLS 1.2 is used due to its widespread adoption in embedded systems and limited TLS 1.3 support in mbedTLS at the time of this study. Additionally, while TLS 1.3 reduces handshake round trips, this advantage is less significant here because post-quantum schemes introduce larger key sizes that already dominate latency.

For cryptographic operations, the NIST P-256 elliptic curve is used for classical ECDHE and ECDSA-based comparisons, with ephemeral keys generated for every session to ensure forward secrecy in both classical and post-quantum configurations. Finally, power consumption and handshake latency are measured using a Nordic Power Profiler Kit 2 and verified with a high-precision Keithley DMM7510 digital multimeter.

3.2 PQC-Based Public Key Encryption

A lightweight public key infrastructure (PKI) was implemented within the IoT environment. In this configuration, both the server and IoT device certificates are issued by a single trusted root certificate authority (CA). Intermediate certificates were intentionally omitted to reduce

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

the amount of certificate chain data exchanged during the TLS handshake, thereby keeping communication overhead minimal.

Apart from standard certificate metadata such as validity period, subject identity, and organization details, the overall size of post-quantum certificates is mainly influenced by the embedded public keys and the digital signature generated by the chosen DSA. In this setup, the server sends its certificate chain—which includes the root and server certificates—to the client, while the client also provides its own certificate to complete the mutual authentication process.

3.3 Software Implementation

TLS security was implemented on both the server and edge devices using post-quantum key exchange mechanisms and digital signature algorithms. The gateway did not require any modifications compared to a standard TLS configuration, as its role is limited to handling communication only at the physical layer without interacting with the cryptographic operations.

3.3.1 Edge Devices

Even though mbedTLS currently supports only TLS 1.2 and not TLS 1.3, it was preferred over wolfSSL for the edge device implementation because of its more permissive licensing terms. The previously customized mbedTLS version from [8] was further enhanced to include support for all NIST Round 3 key encapsulation mechanisms along with the selected digital signature algorithms for use in TLS handshakes. To enable the different PKI configurations described earlier, additional capabilities were added to generate both post-quantum–secure certificates and conventional certificates signed using post-quantum algorithms. The lwIP (Lightweight IP) stack was employed to handle the TCP/IP communication layer.

The PQC algorithms provided by NIST come with reference C implementations, while the pqm4 project [17] offers optimized versions for the ARM Cortex-M4 for most schemes. In this work, pqm4 implementations were used for all KEMs except BIKE and HQC. However, for the digital signature algorithms, the memory requirements of pqm4 exceeded the available RAM in the system, so the original NIST reference implementations were adopted instead. Following the approach in [8], the ARM CryptoCell was utilized to accelerate AES-128 and SHA-2 operations used within PQC constructions, particularly in components such as extendable output functions (XOFs). In addition, SHA-3 was implemented using an assembler-optimized Cortex-M4 version developed by the Keccak team.

3.3.2 Server

The server side uses the open-source Eclipse Mosquitto MQTT broker, which provides an API that enables integration with OpenSSL. For implementing post-quantum security on the server, the TLS 1.2 version of the OQS-OpenSSL library was adopted. Since official support for TLS 1.2 was discontinued by the project in 2020, the library was updated to include the latest versions of the key encapsulation mechanisms.

In addition, the existing library did not provide support for post-quantum digital signature algorithms or certificate handling. To address this limitation, these capabilities were developed and integrated separately to complete the post-quantum TLS functionality on the server.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

4. RESULTS AND DISCUSSION

This section presents the measurement results along with their analysis. The latency and energy consumption of TLS handshakes using post-quantum key encapsulation mechanisms are first evaluated and compared with traditional ECDHE-based handshakes. In addition, the additional overhead introduced by higher-security KEM configurations is examined. The study also analyzes the latency and energy impact of different PKI setups to understand the respective strengths and limitations of the selected digital signature algorithms. Based on these observations, theoretical estimates of battery lifetime for edge devices are derived for various combinations of KEMs and PKI designs.

All experiments were repeated ten times on the client side for each algorithm and PKI configuration. The measurement process covered the complete TLS handshake, beginning with the transmission of the ClientHello message from the edge device and ending upon receipt of the Finished message from the server.

4.1 KEMs

The NIST Round 3 KEMs were integrated into OQS-OpenSSL on the server side and mbed TLS on the client side to evaluate latency, energy consumption, and memory usage in a low-power IoT setup using ECDSA-based PKI.. The results show that TLS 1.2 handshake latency is only minimally affected by the cryptographic computation of most post-quantum KEMs, while the main increase comes from communication overhead due to larger keys and ciphertexts compared to classical ECDHE. Lattice-based schemes such as KYBER, NTRU, SABER, and NTRU-Prime perform best, adding roughly 25% overhead over ECDHE at lower security levels, with energy consumption close to ECDHE even at higher settings, whereas SIKE shows significantly higher energy demand due to computational complexity. Memory analysis indicates that KYBER512 and SIKE_P434 have relatively small stack usage, while code-based KEMs require much larger memory and were limited by resource constraints, and some schemes further increase buffer requirements across mbedTLS and lwIP due to large key sizes. Overall, lattice-based KEMs are shown to be practical for IoT environments, hardware acceleration has limited impact because communication dominates performance, and KYBER512 provides the best trade-off between efficiency and resource usage, making it the preferred choice for further evaluation of DSAs.

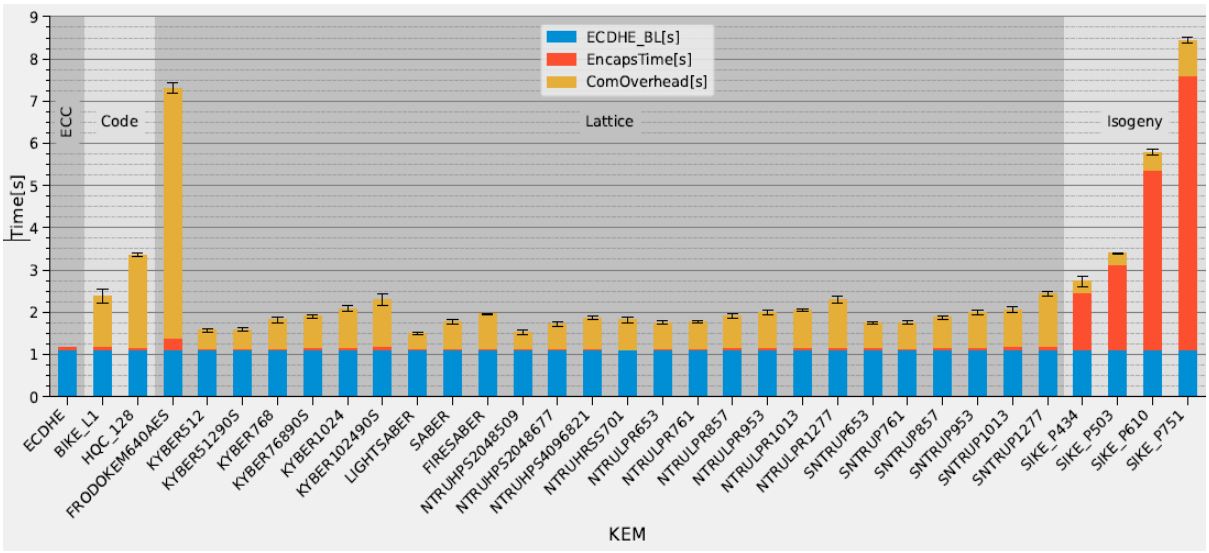

Figure1: TLS1.2 Handshake

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

4.2 DSAs

In alignment with NIST's goal of standardizing a single post-quantum approach[15,16], pq-DSAs were first evaluated using homogeneous PKIs based on individual signature schemes. The study was later extendeed to heterogeneous configurations combining classical and post-quantum algorithms, including mixes of Falcon and Dilithium, since DSAs are invoked multiple times during TLS handshakes and allow greater integration flexibility than KEMs. The results, summarized in Figure 2 using a KYBER512-based ECDSA PKI as the baseline, show that post-quantum DSAs significantly increase TLS handshake latency and energy consumption compared to classical ECDSA, largely due to higher communication overhead from larger keys, signatures, and certificates, as well as computational costs. Dilithium2-based homogeneous PKIs perform worst, with about four times higher latency than ECDSA, mainly due to bandwidth-heavy operations, while Falcon512 reduces latency by roughly half but incurs high signing cost. A hybrid setup using Dilithium2 for client certificates and Falcon512 for server and CA certificates provides a better balance, slightly increasing latency but reducing energy consumption by around 30%. The most efficient configuration combines ECDSA client certificates with Falcon512 server/CA certificates, significantly lowering the overhead compared to fully post-quantum PKIs, indicating that while homogeneous pq-DSA deployments are resource-intensive for IoT devices, carefully designed hybrid PKIs or hardware acceleration for Falcon signing can improve feasibility, with classical client-side certificates still offering a practical transitional solution.

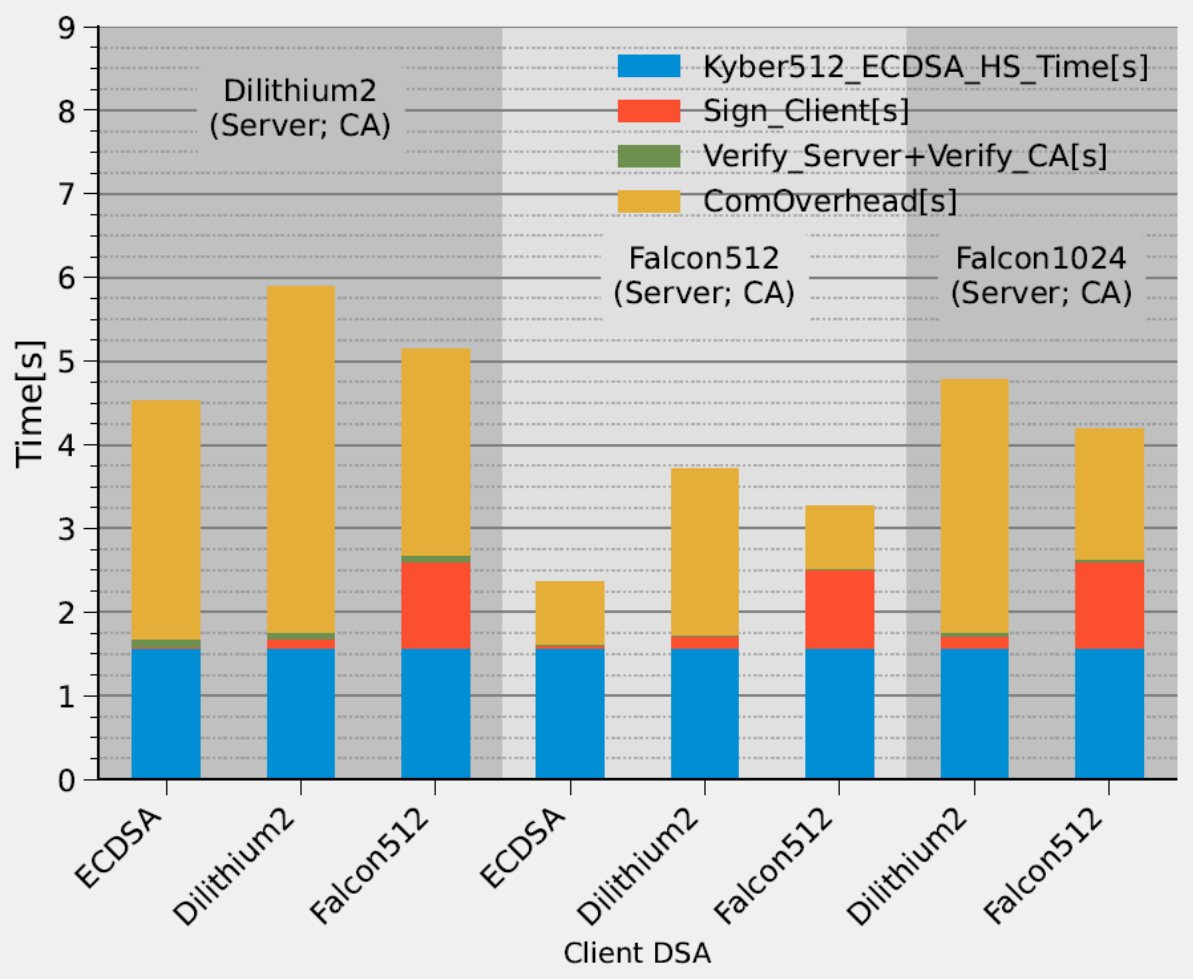

Figure 2: TLS Handshake with Post Quantum DSAs

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

4.3 Battery Life Analysis

Battery lifetime was estimated using a standard 1/2 AA lithium thionyl chloride cell (3.6 V, 1.2 Ah) with a measured sleep current of 2.5 μA, assuming only 70% usable capacity to account for aging effects. Unlike earlier tests focused only on TLS handshakes, this evaluation considers a full TLS-secured MQTT transaction where a small 12-byte encrypted payload is transmitted, representing typical sensor data, while excluding sensor energy costs since they vary by application and are not the focus of this study. The results indicate that most KEMs, including classical ECDHE, show only slight differences in estimated battery life, and even post-quantum schemes introduce limited impact overall. For instance, KYBER512 combined with an ECDSA client certificate and Falcon512 server/CA certificates can still achieve around 10 years of battery life even with over 200 transmissions per day. Even fully Dilithium2-based PKIs reduce lifetime only moderately compared to classical setups, demonstrating that post-quantum TLS-secured communication remains feasible on current IoT hardware without significantly affecting battery longevity while still leaving sufficient energy for sensing and other device operations.

5. CONCLUSION

This work presents a detailed study on the use of post-quantum cryptographic (PQC) algorithms in TLS-secured, low-power IoT systems by extending OpenSSL and mbedTLS to support NIST Round 3 KEMs, digital signature algorithms, and post-quantum–secure certificates suitable for IoT handshakes. Latency, energy consumption, and memory usage of TLS handshakes using quantum-resistant schemes were analyzed within a realistic IoT setup to understand the trade-offs between different algorithms, and also estimated the battery lifetime of edge devices operating under post-quantum secure communication. The results highlight several key findings: a system-level perspective is essential because focusing only on computational cost overlooks important factors like communication overhead, which often dominates performance; PQC can already be effectively deployed on standard IoT hardware, with energy consumption still allowing sufficient capacity for sensing and other tasks, contrary to claims that specialized hardware is always required; the main performance bottleneck comes from large key and signature sizes rather than computation, limiting the benefits of hardware acceleration in most lattice-based schemes and Dilithium, except in cases like Falcon signing or SIKE where computation is more significant; heterogeneous PKI designs that combine different signature schemes (such as Dilithium for clients and Falcon for servers/CA) along with KYBER-based key exchange provide the best balance of energy efficiency, latency, and bandwidth usage, challenging the assumption of using a single standardized algorithm; and finally, hybrid PKI approaches that retain classical ECDSA on some endpoints alongside PQC can significantly reduce overhead while still offering a practical security improvement. Overall, the study demonstrates that post-quantum KEMs and DSAs are already feasible for real-world IoT deployment, with future improvements likely to come from reducing key and signature sizes rather than focusing solely on computational optimizations.

REFERENCES

1. Mades, J., Ebelt, G., Janjic, B., Lauer, F., Rheinländer, C. C., & Wehn, N. (2020, March). TLS-level security for low power industrial IoT network infrastructures. In *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)* (pp. 1720-1721). IEEE.
2. Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science* (pp. 124-134). Ieee.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

3. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready?. *IEEE Security & Privacy*, *16*(5), 38-41.
4. S. (2024). Post-Quantum Cryptography | CSRC. Retrieved April 22, 2026, from Nist.gov website: https://csrc.nist.gov/projects/post-quantum-cryptography
5. Fritzmann, T., Sigl, G., & Sepúlveda, J. (2020). RISQ-V: Tightly coupled RISC-V accelerators for post-quantum cryptography. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 239-280.
6. Nejatollahi, H., Cammarota, R., & Dutt, N. (2019, November). Flexible ntt accelerators for rlwe lattice-based cryptography. In *2019 IEEE 37th International Conference on Computer Design (ICCD)* (pp. 329-332). IEEE.
7. Banerjee, U., Ukyab, T. S., & Chandrakasan, A. P. (2019). Sapphire: A configurable crypto-processor for post-quantum lattice-based protocols. *arXiv preprint arXiv:1910.07557*.
8. Schöffel, M., Lauer, F., Rheinländer, C. C., & Wehn, N. (2021, May). On the energy costs of post-quantum KEMs in TLS-based low-power secure IoT. In *Proceedings of the International Conference on Internet-of-Things Design and Implementation* (pp. 158-168).
9. Stebila, D., & Mosca, M. (2016, August). Post-quantum key exchange for the internet and the open quantum safe project. In *International Conference on Selected Areas in Cryptography* (pp. 14-37). Cham: Springer International Publishing.
10. Paquin, C., Stebila, D., & Tamvada, G. (2020, April). Benchmarking post-quantum cryptography in TLS. In *International Conference on Post-Quantum Cryptography* (pp. 72-91). Cham: Springer International Publishing.
11. mupq. (2024, October 31). GitHub - mupq/pqm4: Post-quantum crypto library for the ARM Cortex-M4. Retrieved April 22, 2026, from GitHub website: https://github.com/mupq/pqm4
12. Saarinen, M. J. O. (2020, August). Mobile energy requirements of the upcoming NIST post-quantum cryptography standards. In *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)* (pp. 23-30). IEEE.
13. Bürstinghaus-Steinbach, K., Krauß, C., Niederhagen, R., & Schneider, M. (2020). Post-quantum TLS on embedded systems. *Cryptology ePrint Archive*.Lauer, F., Rheinländer, C. C., Kestel, C., & Wehn, N. (2020, May). Analysis and optimization of TLS-based security mechanisms for low power IoT systems. In *2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID)* (pp. 775-780). IEEE.
14. Moody, D. (2020). NIST PQC Standardization Update-Round 2 and Beyond. *Online: https://csrc. nist. gov/CSRC/media/Presentations/pqc-update-round-2-and-beyond/images-media/pqcrypto-sept2020-moody. pdf [accessed: April 2021]*.
15. Ramzan, M. T., & Cimato, S. (2025, July). Blockchain in the Quantum Era: Surveying Security Challenges and Post-Quantum Cryptography. In *2025 IEEE 49th Annual Computers, Software, and Applications Conference (COMPSAC)* (pp. 2218-2223). IEEE.
16. Köder, L., Lohmiller, N., Schmieder, P., Buck, B., Menth, M., & Heer, T. (2026). Assessing the Real-World Impact of Post-Quantum Cryptography on WPA-Enterprise Networks. *arXiv preprint arXiv:2601.22892*.