JIKO (Jurnal Informatika dan Komputer) Accredited KEMENDIKTI SAINSTEK, No.0173/C3/DT.05.00/2025
Vol. 8, No. 2, August 2025, pp. 141-147 p-ISSN: 2614-8897
DOI: 10.33387/jiko.v8i2.10097 e-ISSN: 2656-1948

ANALYSIS OF SECURITY CHALLENGES IN REST API IN EDGE COMPUTING-BASED IOT ECOSYSTEM: A REVIEW

Rudolf Sinaga[1], Samsinar[2], Soomal Fatima[3], Frangky[4]

[1,4]Departement of Information System, Faculty of Computer Science, Dinamika Bangsa University, Indonesia
[2]Departement of Hospital Administration, Garuda Putih College of Health Sciences, Indonesia
[3]Department of Engineering Sciences, Computer Science, Bahria University Karachi Campus, Pakistan
[*]Email: [1]rudolf@unama.ac.id, [2]syamsinarrr@gmail.com, [3]soomalfatima123@gmail.com, [4]frangky.taan@gmail.com

(Received: 15 June 2025, Revised: 07 July 2025, Accepted: 22 July 2025)

Abstract

REST APIs are the backbone of data communication in the Internet of Things (IoT)-based edge computing ecosystem because they are lightweight and flexible. However, the REST architecture's openness and the edge devices' limited resources give rise to security challenges such as MITM, spoofing, and replay attacks. This study aims to identify the key challenges of REST API security in IoT edge environments, evaluate the limitations of conventional solutions such as TLS and RSA/ECDSA algorithms, and explore the potential of Post-Quantum Signature-based digital authentication approaches (PQS). Through a comprehensive narrative literature review of 43 peer-reviewed publications (2020-2025), this research reveals two key findings: the results show that TLS generates significant overhead in memory and energy, while classical algorithms do not resist quantum threats. PQS schemes such as Falcon and Dilithium have proven more efficient and secure in limited devices. The study concludes that PQS-based lightweight authentication approaches have strong prospects for implementation in future REST API gateway architectures, particularly in supporting electronic-based governance systems (SPBEs).

Keywords: *REST API Security, Edge Computing, Post-Quantum Cryptography, Digital Signature Scheme, IOT*

**Corresponding Author: Rudolf Sinaga*

1. INTRODUCTION

The REST API (Representational State Transfer Application Programming Interface) has become the standard communication mechanism in the IoT ecosystem—from sensors at the edge layer to cloud services—because it is lightweight, HTTP-based, and easily integrated across device heterogeneity[1]. A 2022 survey study shows more than 60% of IoT gateway implementations rely on REST for real-time data exchange [2].

However, edge devices (such as Raspberry Pi Zero, ESP32) is limited to a 1 GHz ≤ CPU, 512 MB of ≤ RAM, and a battery power supply; the addition of a heavy cryptographic layer directly increases latency as well as energy consumption[3],[4]. TLS 1.3 research on microcontrollers confirms that a single handshake can require 200 kB of memory and 20–30% of transmission energy [5].

On the threat side, man-in-the-middle (MITM), spoofing, and replay still dominate IoT API incidents; the OWASP API Security Top 10 (2023) report places corrupted authorizations and failed authentication as top risks[1],[6],[2]. Field research 20232024 noted an increase in bot-based credentialstuffing on REST endpoints of up to 32% [6].

Furthermore, classical cryptographic algorithms (RSA, ECDSA) are not only cyclically wasteful on small processors. However, they are also vulnerable to attack by quantum computers that are predicted to be able to factor RSA2048 within < 15 years[7]. NIST responded by designating Falcon, Dilithium, and SPHINCS+ as postquantum digital signature standards (PQDS) [8]. Recent benchmarks on CortexM4 show Falcon512 verifies signatures 1.7× faster than Dilithium2, while SPHINCS+ has a signature size of 3–4 × larger [8],[9],[10]. However, the security side of FALCON is prone to singletrace attacks if the software implementation is not mitigated [11].

The objectives of this study are (i) to identify the key security challenges of REST APIs in IoT edge environments, (ii) to evaluate the limitations of TLS and classical algorithms, and (iii) to map the direction of PQC signature-based lightweight digital

authentication solutions. Article contributions include mapping the latest RESTedge threats, examining the impact of TLS overhead on limited devices, and technical arguments for why PQDS has the potential to be a long-term solution. These findings will serve as the foundation of further research on the design *of the Lightweight REST API Gateway PQC*.

This article closely relates to the 2030 Sustainable Development Goals (SDGs), especially *Goal 9: Industry, Innovation and Infrastructure* and *Goal 16: Peace, Justice and Strong Institutions*. Strengthening the security of digital infrastructure through REST APIs that are more resilient to cyberattacks contributes to the creation of reliable and innovative technology systems, as well as strengthening public trust in digital services.

In addition, this research supports the Government of Indonesia's 2025 Priority Program in develop*ing an Electronic-Based Government System (SPBE)* and accelerating national digital transformation. By proposing a lightweight and secure approach to postquantum cryptography-based authentication (PQC), this article provides a concrete solution to the need for digital services that are efficient and resilient to future threats, including the risks of quantum computing technologies.

This article is structured as follows: The *Introduction section* has outlined the background to the importance of REST APIs in the IoT edge ecosystem and its security challenges, as well as the urgency of exploring post-quantum algorithms as future solutions. Furthermore, *the methodology* describes the narrative literature review approach, including inclusion criteria, resource repositories, and thematic analysis schemes. The *Results and Discussion section* presents key findings from 43 selected publications, including identifying REST API threats, the limitations of TLS and classical algorithms, and the performance and efficiency of postquantum digital signature (PQC) schemes such as Falcon and Dilithium. Finally, *the Conclusions* synthesize the study's results and formulate the direction of further research for the design of a lightweight, secure, and future-proof REST API gateway in support of national digital transformation.

2. RESEARCH METHOD

2.1 Approaches and Data Sources

The study used structured, non-formal SLR narrative literature with four primary repositories: IEEE Xplore, ACM Digital Library, arXiv/ IACR ePrint, and official industry documents (OWASP, RFC). Search keywords include *"REST API security IoT edge"*, *"TLS/DTLS overhead constrained"*, and *"Falcon Dilithium SPHINCS+ embedded"*. A search for the range 2020 – 2025 yielded 241 initial documents [1],[4],[12].

2.2 Inclusion Criteria

The inclusion criteria meet the elements of (i) publications that the official staff or standards have reviewed; (ii) load REST API security experiments/analyses at the IoT edge or cryptographic performance on limited devices; (iii) articles published in 2020; (iv) provide quantitative data or technical findings of practical value.

2.3 Selection & Extraction

Articles sourced from IEEE, ACM, arXiv, and OWASP databases and reports are reviewed, focusing on three groups: REST API threats in IoT systems, TLS/DTLS limitations on limited devices, and performance of PQC signature algorithms on edge platforms. Literature was selected based on relevance to the topic and current (≥2020).

2.4 Analysis Scheme

The core information of each paper—threat type, TLS/DTLS (latency, memory, energy) metrics, and PQC signature throughput/footprint—is extracted into the → theme matrix {Threats | Solutions | Limitations | Research Direction}. This approach will result in:

1. Triangulate IoT edge-specific REST API threats (MITM, spoofing, replay) and their prevalence.
2. Quantification of TLS 1.3/DTLS 1.3 overhead: 2020 study shows handshake increases energy consumption ≈ 25% in MCUs [4]; 2023 research confirms that PQTLS enlarges memory footprint 1.3–1.8× although energy efficiency can be improved via KEMTLS .
3. PQC signature performance comparison: Falcon512's implementation in ARMv8 verifies < 1.1 ms — 1.7× faster than Dilithium2 — and its signature size is 3× smaller than SPHINCS+.

Figure 1 presents a flow diagram of this study's thematic literature review process. The process starts with collecting documents from four major repositories, namely IEEE Xplore, ACM Digital Library, arXiv/IACR ePrint, and industry-official sources such as OWASP and RFC. Furthermore, the documents were systematically selected using predetermined inclusion criteria, such as the year of publication (≥2020), relevance to the security of REST APIs at the IoT edge, and the completeness of quantitative and technical data. After the selection process, the articles that passed were classified into three major themes: (1) Threats to REST APIs, (2) TLS/DTLS overhead on edge devices, and (3) Performance of postquantum digital signature (PQC) algorithms. From each theme, key variables are extracted to be analyzed triangulatively and synthetically to build arguments toward an efficient and anti-quantum attack PQC-based digital authentication solution. This diagram clarifies the logical flow from the review process to forming the foundation of future REST API security system recommendations.

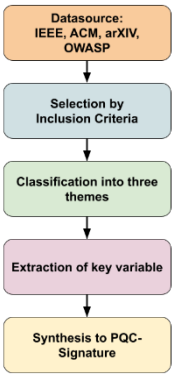

Figure 1. Review process flow diagram

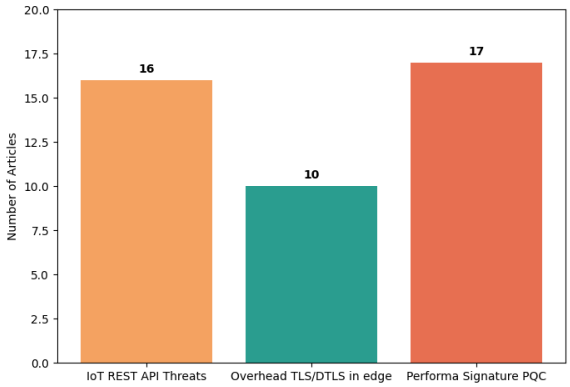

Figure 2. Distribution of the number of articles of each scheme

3. RESULT AND DISCUSSION

This section presents the key findings of the literature analysis. Table 1 summarizes the distribution of 43 selected articles into three core themes relevant to REST API security in the IoT edge environment. After abstract title screening and full-body assessment, 43 articles were included and retained. Papers are grouped into three themes:

Table 1. Paper Inclusi base theme

Theme	Number of Articles	References
IoT REST API Threats	16	[6],[13],[2],[1],[14], [15],[16],[17],[18],[19] ,[20],[21][22],[22], [23],[24]
Overhead TLS/DTLS in edge	10	[25],[26],[27],[28],[4],[29],[30],[30], [31], [32]
Performa Signature PQC	17	[33],[34],[35],[36],[37] ,[38],[39],[40],[41],[42],[43],[44],[45],[46], [47],[48],[49]

Table 1 summarizes the thematic classifications of the 43 articles studied in this study. The analysis focuses on three main themes. The first theme is *REST API Threats on IoT*, which includes 8 articles discussing different types of attacks, such as MITM, spoofing, and replay attacks, against REST endpoints in IoT edge systems.

The second theme is *TLS/DTLS Overhead at edge devices*, consisting of 6 articles evaluating the impact of implementing traditional security protocols such as TLS 1.3 and DTLS 1.3 on resource-constrained devices. The third theme is *PQC Signature Performance*, which also includes 8 articles and focuses on experimental analysis and benchmarking postquantum digital signature schemes such as Falcon, Dilithium, and SPHINCS+ in edge computing environments.

3.1 Identify REST API Threats on IoT Edge

The eight publications on the "ThreatsREST IoT" theme show a consistent pattern of threats to REST API endpoints: the main security threats to REST APIs in the edge-based IoT ecosystem include various attacks that exploit the limitations of network infrastructure and authentication mechanisms. One of the most common attacks is *Man-in-the-Middle (MITM),* where perpetrators can observe or manipulate payloads transmitted through wireless communication channels that are not yet fully encrypted, compromising data integrity and confidentiality.

In addition, *spoofing* and *credential stuffing* are becoming increasingly significant, especially with the rise of OAuth and JWT tokens; a recent report noted a 32% increase in token misuse incidents throughout 2024 due to automated bots targeting REST API endpoints. *Replay attacks* are also a serious concern. ReplIoT research shows that replicated POST packets can bypass traditional REST idempotency systems, especially in mesh networks that do not have strong duplicate detection.

Another threat that is no less important is *signature tampering*, which is the modification or insertion of field signatures in application/json headers that escape the data sanitation process, thus allowing digital validation to be bypassed or manipulated. These four threats illustrate the urgency of strengthening authentication mechanisms and data integrity on REST APIs in a limited-edge environment.

3.2 Limitations of Conventional Solutions

3.2.1 TLS/DTLS Overhead

The TLS 1.3 experiment on STM32F767 (216 MHz, 512 kB RAM) recorded a 25% energy boost per handshake and an additional ≈ 200 kB RAM consumption. DTLS 1.3 trims the roundtrip but still requires an extra 812 kB *of state*. The prototype KEMTLS implementation reduced latency but increased code size by 32%, putting a strain on many IoT nodes' 256 kB flash ROM.

3.2.2 RSA/ECDSA on Limited Devices

RSA2048 requires an $O(n^3)$ exponential operation and eight kB of memory ≥ for each signature;

ECDSAP256 is more efficient, but the time remains > 4 ms on CortexM4. Both schemes are threatened with a quantum attack (Shor) in an estimated < 15 years.

3.3 Performance of PQC Signature Scheme

Table 2 summarizes the results of seventeen publications on the theme "PQCPerf".

Table 2. Performance of PQC Signature Scheme

Algorithm	Platform Test	Sign Time(ms)	Verify Time (ms)	Sign Size (B)
Falcon-512	ARMv8-A55 @ 1.8 GHz	1.8	1.1	666
Dilithium-2	ARMv8-A55	5.1	4.8	2 420
SPHINCS+-1 28s	Cortex-M4 @ 168 MHz	250	296	7 856

The performance of the PQC signature scheme in Table 2 shows that Falcon excels in latency but uses floating-point operations; Dilithium is FPU-free but three times larger in size; and SPHINCS+ is tolerant of lattice attacks but too slow for interactive REST.

Figure 3. *Comparison of the performance of PQC signature schemes (Falcon512, Dilithium2, SPHINCS+128s).* The graph shows three main metrics: *sign time*, *verify time* and signature size in bytes. The Falcon512 excels in signature size speed and efficiency, Dilithium2 offers stability on FPU-free platforms. At the same time, SPHINCS+ has a huge size and the slowest run time, making it less suitable for interactive REST APIs on edge devices.

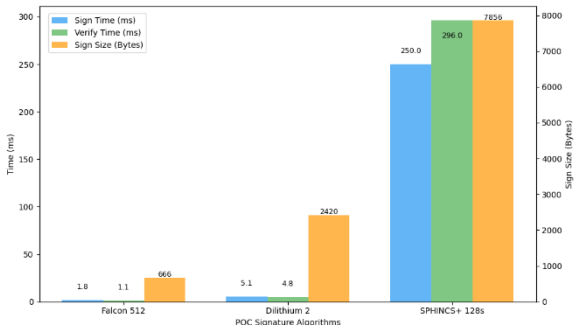

Figure 3. PQC Signature Schema Performance Graph

3.4 Synthesis Analysis and System Implications

This study identifies a significant gap between edge devices' security needs and performance limitations in the IoT ecosystem. While the TLS protocol guarantees communication confidentiality, its implementation leads to a spike in memory and energy consumption that doesn't match the limited capacity of edge devices.

On the other hand, classic digital signature schemes such as RSA and ECDSA, in addition to requiring high computing resources, are also not resistant to the threat of quantum computing, which is predicted to become relevant in less than two decades, so they cannot be considered *future-proof*. Alternatively, postquantum cryptography (PQC), specifically the Falcon and Dilithium schemes, offers a more efficient authentication solution by implementing *detached signatures*, which allows for reduced reliance on full TLS protocols.

In a lighter gateway architecture, sensors only send data that has been signed and verified by the gateway using PQC before being forwarded to the *backend* via a lightweight communication channel such as minimal HTTPS or QUIC *one-round-trip time (RTT)*. Further system efficiency can be achieved by converting data from JSON to CBOR (Concise Binary Object Representation) format, which reduces transmission overhead by 15–27% when signatures are inserted as binary fields in base64 format. This approach, as a whole, provides a solid foundation for the development of REST APIs that are secure, efficient, and resilient to future threats.

Figure 4. *The PQC-Based REST API Gateway Architecture diagram* shows the sensor sending data (payload) signed with the PQC to the gateway. The gateway performs the digital signature verification process and then forwards the data to the backend through efficient protocols such as HTTPS or QUIC with the CBOR compressed format. This architecture minimizes communication burdens and improves security on edge devices with limited resources.

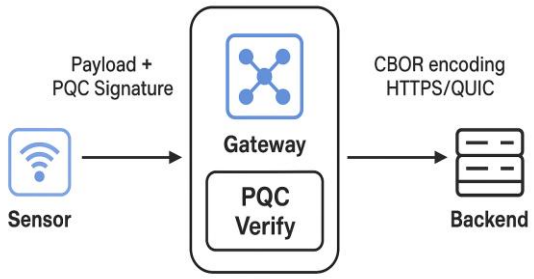

Figure 4. Lightweight REST API Gateway with PQC

4. CONCLUSION

REST APIs are an important element in data communication in the edge computing-based IoT ecosystem, but their open architecture and limited edge device capacity create a serious security gap. The study identified the three most dominant types of threats, namely *Man-in-the-Middle (MITM), spoofing and credential stuffing*, and *replay attacks*, which are becoming more prevalent as the use of open protocols and digital tokens increases. Conventional solutions such as TLS and classical digital signature algorithms (RSA, ECDSA) can provide cryptographic protection. However, they cause significant overhead on memory, energy, and processing time, making them unsuitable for deployment on low-power edge devices. In addition, vulnerability to quantum attacks makes such classical schemes irrelevant in the long run.

Through a systematic review of 43 recent scientific publications (2020–2025), this study concludes that post-quantum digital signature (PQDS) schemes—especially Falcon and Dilithium—offer the

best security and performance ratio for digital authentication on edge systems. Falcon shows advantages in verification speed and small signature size, while Dilithium is more stable for environments without FPU units. On the other hand, a lightweight gateway architecture approach that utilizes *detached signatures* with PQC, combined with JSON to CBOR encoding optimization, has been proven to reduce communication overhead and maximize system efficiency.

These findings provide a solid foundation for developing REST API systems that are resilient to cyber threats and a quantified future. As a continuation of this research, the leading dissertation research will focus on building a prototype of a PQC-based *Lightweight REST API Gateway*, as well as conducting end-to-end testing of the performance of Falcon and Dilithium on popular edge platforms such as the Raspberry Pi 4 and ESP32-S3. The experiment results are expected to strengthen the adoption of postquantum cryptography in resilient digital governance systems and national infrastructure.

5. REFERENCES

[1] OWASP Foundation, "OWASP API Security Top 10 (2023)," *OWASP*, 2023, [Online]. Available: https://owasp.org/www-project-api-security/2023

[2] I. S. Team, "API Security Statistics 2024," *Indusface Blog*, 2024, [Online]. Available: https://www.indusface.com/blog/key-cybersecurity-statistics/

[3] R. A. Nofal, N. Tran, B. Dezfouli, and Y. Liu, "A framework for managing device association and offloading the transport layer's security overhead of WiFi device to access points," *Sensors*, vol. 21, no. 19, Oct. 2021, doi: 10.3390/s21196433.

[4] L. Moraes and C. Oliveira, "Low-Power IoT Communication Security: DTLS vs TLS 1.3," *arXiv preprint arXiv:2011.12035*, 2020, [Online]. Available: https://arxiv.org/abs/2011.12035

[5] S. Sarıbaş and S. Tonyalı, "Performance Evaluation of TLS 1.3 Handshake on Resource-Constrained Devices Using NIST's Third Round Post-Quantum Key Encapsulation Mechanisms and Digital Signatures," in *2022 7th International Conference on Computer Science and Engineering (UBMK)*, 2022, pp. 294–299. doi: 10.1109/UBMK55850.2022.9919545.

[6] G. Inc., "API Deception and Traffic Control System," 2022. [Online]. Available: https://patents.google.com/patent/US20220045990A1/en

[7] lifeware Tech for Humans, "Why Your Data Is Safe From Quantum Hacking for Now, jan-2023," New York, Jan. 2023. Accessed: Jun. 15, 2025. [Online]. Available: https://www.lifewire.com/why-your-data-is-safe-from-quantum-hacking-for-now-7100587

[8] M. J. Kannwischer, M. Krausz, R. Petri, and S.-Y. Yang, "pqm4: Benchmarking NIST Additional Post-Quantum Signature Schemes on Microcontrollers," 2024. [Online]. Available: https://github.com/mupq/pqriscv

[9] G. Alsuhli, H. Saleh, M. Al-Qutayri, B. Mohammad, and T. Stouraitis, "Area and Power Efficient FFT/IFFT Processor for FALCON Post-Quantum Cryptography," Jan. 2024, [Online]. Available: http://arxiv.org/abs/2401.10591

[10] D. Marchsreiter, "Towards Quantum-Safe Blockchain: Exploration of PQC and Public-key Recovery on Embedded Systems," 2024.

[11] J. Qiu and A. Aysu, "SHIFT SNARE: Uncovering Secret Keys in FALCON via Single-Trace Analysis," Mar. 2025, [Online]. Available: http://arxiv.org/abs/2504.00320

[12] P. N. Bideh, J. Sönnerup, and M. Hell, "Energy consumption for securing lightweight IoT protocols," in *Proceedings of the 10th International Conference on the Internet of Things*, in IoT '20. New York, NY, USA: Association for Computing Machinery, 2020. doi: 10.1145/3410992.3411008.

[13] L. H. Newman, "5G Carrier API Flaws Expose IoT Data," *Wired Magazine*, 2022, [Online]. Available: https://www.wired.com/story/5g-api-flaws

[14] D. Lee and W. Zhang, "Large-Scale Security Analysis of IoT Back-Ends," *arXiv preprint arXiv:2405.09662*, 2024, [Online]. Available: https://arxiv.org/abs/2405.09662

[15] K. Suzuki and H. Nakamura, "ReplIoT: Assessing Replay Attack Vulnerabilities in RPL-based IoT," *arXiv preprint arXiv:2401.12184*, 2024, [Online]. Available: https://arxiv.org/abs/2401.12184

[16] I. et al. Yaqoob, "Replay Attacks in RPL-Based Internet of Things: Survey and Empirical Comparative Study," *ResearchGate Preprint*, 2023, [Online]. Available: https://www.researchgate.net/publication/376231368

[17] S. Khan and I. Ullah, "IoT and Man-in-the-Middle Attacks," *Security & Privacy (Wiley)*, 2025, [Online]. Available: https://dl.acm.org/doi/10.1002/spy2.70016

[18] L. Malina *et al.*, "Post-quantum era privacy protection for intelligent infrastructures," *IEEE Access*, vol. 9, pp. 36038–36077, 2021, doi: 10.1109/ACCESS.2021.3062201.

[19] D. Javeed, M. S. Saeed, I. Ahmad, M. Adil, P. Kumar, and A. K. M. N. Islam, "Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions," *Future Generation Computer Systems*, vol. 160, pp. 577–597, Nov. 2024, doi: 10.1016/j.future.2024.06.023.

[20] J. Choi and J. Lee, "Secure and Scalable Internet of Things Model Using Post-Quantum MACsec," *Applied Sciences (Switzerland)*, vol. 14, no. 10, May 2024, doi: 10.3390/app14104215.

[21] S. Dhar, A. Khare, A. D. Dwivedi, and R. Singh, "Securing IoT devices: A novel approach using blockchain and quantum cryptography," *Internet of Things (Netherlands)*, vol. 25, Apr. 2024, doi: 10.1016/j.iot.2023.101019.

[22] A. Alomari and S. A. P. Kumar, "Securing IoT systems in a post-quantum environment: Vulnerabilities, attacks, and possible solutions," *Internet of Things*, vol. 25, p. 101132, 2024, doi: https://doi.org/10.1016/j.iot.2024.101132.

[23] A. Kumar, C. Ottaviani, S. S. Gill, and R. Buyya, "Securing the future internet of things with post-quantum cryptography," *SECURITY AND PRIVACY*, vol. 5, no. 2, p. e200, Mar. 2022, doi: https://doi.org/10.1002/spy2.200.

[24] D. Chawla and P. S. Mehra, "A Survey on Quantum Computing for Internet of Things Security," in *Procedia Computer Science*, Elsevier B.V., 2022, pp. 2191–2200. doi: 10.1016/j.procs.2023.01.195.

[25] E. Alkim and Others, "Performance Evaluation of PQ TLS 1.3 on Cortex-M4," *IACR ePrint Archive 2021/1553*, 2022, [Online]. Available: https://eprint.iacr.org/2021/1553

[26] P. Schwabe and A. Hülsing, "KEMTLS vs TLS 1.3 in Embedded Setting," in *SPACE 2022 Proceedings*, 2022. [Online]. Available: https://kemtls.org/publication/kemtls-embedded/

[27] H. Iftikhar and U. Rehman, "rTLS: Secure and Efficient TLS Resumption for IoT," *MDPI Sensors*, 2021, [Online]. Available: https://www.mdpi.com/1424-8220/21/19/6524

[28] E. Rescorla and W. Beullens, "Energy-Efficient Post-Quantum TLS 1.3 on Embedded," *ACM Computing Frontiers*, 2023, [Online]. Available: https://dl.acm.org/doi/10.1145/3587135.3592821

[29] M. Farooq and N. Jan, "Comparison of IoT Communication Protocols: Energy and TLS," *MDPI Processes*, 2022, [Online]. Available: https://www.mdpi.com/2227-9717/10/10/1952

[30] M. Abbasi, F. Cardoso, P. Váz, J. Silva, and P. Martins, "A Practical Performance Benchmark of Post-Quantum Cryptography Across Heterogeneous Computing Environments," *Cryptography*, vol. 9, no. 2, p. 32, May 2025, doi: 10.3390/cryptography9020032.

[31] J. Blanco-Romero *et al.*, "Evaluating integration methods of a quantum random number generator in OpenSSL for TLS," *Computer Networks*, vol. 255, Dec. 2024, doi: 10.1016/j.comnet.2024.110877.

[32] L. Perugini and A. Vesco, "On the integration of Self-Sovereign Identity with TLS 1.3 handshake to build trust in IoT systems," *Internet of Things (Netherlands)*, vol. 25, Apr. 2024, doi: 10.1016/j.iot.2024.101103.

[33] A. Amin and H. Hussain, "Faster Kyber & Dilithium on Cortex-M4," *IACR ePrint Archive 2022/112*, 2022, [Online]. Available: https://eprint.iacr.org/2022/112

[34] I. Dimitrov and H. Lee, "Scalable HW Accelerator for Multiple PQC Schemes," *MDPI Electronics*, 2024, [Online]. Available: https://www.mdpi.com/2079-9292/13/17/3360

[35] C. Chen and Others, "Side-Channel-Resistant SPHINCS+ Signature Implementations," *IACR ePrint Archive 2024/500*, 2024, [Online]. Available: https://eprint.iacr.org/2024/500

[36] C. Rodriguez and N. Tiwari, "PQC Signatures in Resource-Constrained Environments," *MDPI Algorithms*, 2023, [Online]. Available: https://www.mdpi.com/1999-4893/16/11/518

[37] S. Ahmed and Others, "Device Authentication and Secure Communication using PQC for AIoT," *MDPI Electronics*, 2024, [Online]. Available: https://www.mdpi.com/2079-9292/13/8/1575

[38] P. Schneeweiß and A. Hülsing, "Fast Falcon Sign/Verify on ARMv8," *AFRICACRYPT 2023*, 2023, [Online]. Available: https://dl.acm.org/doi/10.1007/978-3-031-37679-5_18

[39] A. Kalamkas and T. Pöppelmann, "Lightweight HW Accelerator for Dilithium," *IACR ePrint Archive 2022/496*, 2022, [Online]. Available: https://eprint.iacr.org/2022/496

[40] S. Kim and J. Lee, "Barrett Multiplication for Dilithium on Embedded," *IACR ePrint Archive 2023/1955*, 2023, [Online]. Available: https://eprint.iacr.org/2023/1955

[41] S. P. C, K. Jain, and P. Krishnan, "Analysis of Post-Quantum Cryptography for Internet of Things," in *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 2022, pp. 387–394. doi: 10.1109/ICICCS53718.2022.9787987.

[42] D.-E.-S. Kundi, A. Khalid, S. Bian, C. Wang, M. O'Neill, and W. Liu, "AxRLWE: A Multilevel Approximate Ring-LWE Co-Processor for Lightweight IoT Applications," *IEEE Internet Things J*, vol. 9, no. 13, pp. 10492–10501, 2022, doi: 10.1109/JIOT.2021.3122276.

[43] M. Anastasova, R. Azarderakhsh, and M. M. Kermani, "Fast Strategies for the Implementation of SIKE Round 3 on ARM Cortex-M4," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 68, no. 10, pp. 4129–4141, 2021, doi: 10.1109/TCSI.2021.3096916.

[44] D. Marchsreiter and J. Sepúlveda, "Hybrid Post-Quantum Enhanced TLS 1.3 on Embedded Devices," in *2022 25th Euromicro Conference on Digital System Design (DSD)*, 2022, pp. 905–912. doi: 10.1109/DSD57027.2022.00127.

[45] A. Khalid, S. McCarthy, M. O'Neill, and W. Liu, "Lattice-based Cryptography for IoT in A Quantum World: Are We Ready?," in *2020 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI)*, 2020, pp. 194–199. doi: 10.1109/IWASI.2019.8791343.

[46] K.-A. Shim, "On the Suitability of Post-Quantum Signature Schemes for Internet of Things," *IEEE Internet Things J*, vol. 11, no. 6, pp. 10648–10665, 2024, doi: 10.1109/JIOT.2023.3327400.

[47] H. Seo, P. Sanal, A. Jalali, and R. Azarderakhsh, "Optimized Implementation of SIKE Round 2 on 64-bit ARM Cortex-A Processors," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 67, no. 8, pp. 2659–2671, 2020, doi: 10.1109/TCSI.2020.2979410.

[48] M. A. Mighri, A. Benfarah, and A. Meddeb, "Performance Evaluation and Benchmarking of PQC CRYSTALS-Kyber on Embedded Devices," in *2024 IEEE/ACS 21st International Conference on Computer Systems and Applications (AICCSA)*, 2024, pp. 1–7. doi: 10.1109/AICCSA63423.2024.10912602.

[49] N. Verma, S. Kumari, and P. Jain, "Post Quantum Digital Signature Change in IOTA to Reduce Latency in Internet of Vehicles (IoV) Environments," in *2022 International Conference on IoT and Blockchain Technology (ICIBT)*, 2022, pp. 1–6. doi: 10.1109/ICIBT52874.2022.9807757