ARTÍCULOS DE REVISIÓN

Post-Quantum Security Frameworks for Internet of Things Systems: A Layered Narrative Review of Architectures, Protocols, Trust, and Emerging Challenges

Rodrigo Jara Espinoza
https://orcid.org/0009-0004-0811-9206
20224280@aloe.ulima.edu.pe
Laboratorio SAP, Universidad de Lima, Perú

Yohamin Nafit Pimentel Alarcon
https://orcid.org/0009-0006-8068-2874
20215176@aloe.ulima.edu.pe
Laboratorio SAP, Universidad de Lima, Perú

Angelo Taco-Jimenez
https://orcid.org/0000-0001-9806-5379
ataco@ulima.edu.pe
Universidad de Lima, Perú

Fabricio Martin Chavez Rodriguez
https://orcid.org/0009-0002-6080-7642
20224387@aloe.ulima.edu.pe
Laboratorio SAP, Universidad de Lima, Perú

Received: May 16, 2026 / Accepted: June 15, 2026
doi: https://doi.org/10.26439/interfases2026.n023.8810

ABSTRACT. Quantum computing poses a significant threat to classical asymmetric cryptography, which is essential for ensuring confidentiality, authentication, and key exchange in contemporary digital infrastructures. Although post-quantum cryptography (PQC) provides mechanisms that resist quantum attacks, its implementation in Internet of Things (IoT) systems is challenged by constrained resources, including limitations in computation, memory, energy, latency, and bandwidth, and the heterogeneity of devices. This paper offers a comprehensive narrative review of PQC approaches applicable to IoT, systematically organizing 30 peer-reviewed studies published between 2022 and 2026 across four layers: device, communication, distributed trust, and application. Additionally, the review examines two cross-cutting dimensions, privacy and side-channel resistance. The analysis indicates a significant prevalence of lattice-based schemes, hybrid strategies, and integrations with blockchain technology, zero-knowledge proofs, federated learning, homomorphic

encryption, AI, and Zero Trust architectures. Notably, key gaps remain in side-channel evaluation, migration pathways, deployment costs, and real-world validation—issues that are particularly critical given the long lifecycles of IoT devices and the ongoing threat of "harvest now, decrypt later" attacks.

Keywords: post-quantum cryptography / Internet of Things / lattice-based cryptography / side-channel attacks / privacy

MARCOS DE SEGURIDAD POSCUÁNTICA PARA SISTEMAS DE LA INTERNET DE LAS COSAS: UNA REVISIÓN NARRATIVA ESTRATIFICADA DE ARQUITECTURAS, PROTOCOLOS, CONFIANZA Y DESAFÍOS EMERGENTES

RESUMEN. La computación cuántica representa una amenaza para la criptografía asimétrica clásica, que sustenta la confidencialidad, autenticación e intercambio de claves en las infraestructuras digitales modernas. Si bien la criptografía poscuántica (PQC) ofrece mecanismos resistentes a adversarios cuánticos, su despliegue en sistemas IoT se ve dificultado por recursos limitados —cómputo, memoria, energía, latencia y ancho de banda— y la heterogeneidad de dispositivos. Este artículo presenta una revisión narrativa de enfoques PQC para IoT, organizando treinta estudios revisados por pares (2022-2026) en cuatro capas (dispositivo, comunicación, confianza distribuida y aplicación) y dos dimensiones transversales (privacidad y resistencia a ataques de canal lateral). El análisis revela una predominancia de esquemas basados en retículos, estrategias híbridas e integraciones con blockchain, pruebas de conocimiento cero, aprendizaje federado, cifrado homomórfico, IA y arquitecturas Zero Trust. Las brechas abiertas más relevantes incluyen la evaluación de canales laterales, rutas de migración, costos de despliegue y validación en entornos reales —aspectos críticos dado el largo ciclo de vida de los dispositivos IoT y la amenaza activa de ataques *harvest now, decrypt later*.

PALABRAS CLAVE: criptografía poscuántica / internet de las cosas / criptografía basada en retículas / ataques de canal lateral / privacidad

1. INTRODUCTION

Quantum computing presents a significant challenge to the security of digital systems, primarily due to its potential to undermine classical asymmetric cryptography. In response to this threat, post-quantum cryptography has emerged as a viable approach to maintaining essential guarantees such as confidentiality, authentication, and integrity in the face of adversaries equipped with quantum capabilities. Transitioning to post-quantum cryptography within Internet of Things (IoT) systems is particularly complex, as these devices and networks frequently operate under constraints related to computation, memory, energy, latency, and bandwidth. Furthermore, the high degree of heterogeneity in platforms, protocols, and application domains exacerbates this challenge. As a result, migrating to post-quantum cryptography in IoT encompasses not only cryptographic concerns but also significant architectural and operational complexities.

Recent literature examines post-quantum security in IoT from a variety of perspectives. These include key encapsulation mechanisms, digital signatures designed for constrained hardware, the integration of post-quantum cryptography (PQC) into protocols and handshakes, post-quantum authentication, blockchain-based trust, privacy-preserving computation, federated learning, homomorphic encryption, and zero-knowledge proofs, among others. However, these contributions remain scattered across various technical layers, application domains, platforms, and evaluation criteria. This diversity underscores that the transition to PQC involves more than merely replacing vulnerable algorithms; it necessitates a thorough analysis of how new cryptographic primitives impact the device, communication, trust, and application levels of IoT systems. Consequently, a narrative synthesis is essential for organizing these approaches, identifying common patterns, and determining existing research gaps.

This review presents a narrative survey rather than a systematic literature review. It intentionally avoids exhaustive coverage or a formal screening protocol, aiming instead for a thematically coherent synthesis of recent peer-reviewed studies. The review organizes post-quantum security approaches into a layered analytical architecture comprising four functional layers: the device, communication, distributed trust, and application layers. Additionally, it incorporates the cross-cutting dimensions of privacy and resistance to side-channel attacks. This organization does not constitute a definitive taxonomy; rather, it serves as an analytical framework for comparing diverse contributions within a unified structure.

The contributions of this review are threefold. First, it systematically organizes recent studies on PQC-IoT based on the functional levels at which post-quantum mechanisms are implemented. Second, it delineates the primary cryptographic families and enabling technologies addressed in the literature, including lattice-based, hash-based, code-based, hybrid, blockchain-based, zero-knowledge, federated learning, and homomorphic encryption approaches. Third, it highlights persistent gaps concerning side-channel resistance,

longitudinal migration, operational deployment costs, and validation within real-world IoT environments.

This article employs a narrative review design in Section 2 and presents a conceptual framework in Section 3. In Sections 4 through 6, the authors describe the layered analysis, and in Section 7, they provide a comparative synthesis. The conclusions are explained in Section 8.

2. NARRATIVE REVIEW DESIGN AND CORPUS CONSTRUCTION

This study utilizes a narrative survey design rather than a systematic review. It does not employ a reproducible screening protocol; instead, it constructs a thematically selected corpus to organize diverse contributions and identify recurring research gaps. This approach is suitable given the field's diversity, which encompasses optimization of cryptographic primitives, blockchain technology, federated learning, artificial intelligence, edge computing, homomorphic encryption, and zero-knowledge proofs.

An exploratory search was conducted in the databases Scopus, IEEE Xplore, and Web of Science (initially accessed February 10, 2026), focusing on publications from 2021 to 2026. The search parameters included articles published in English, categorized under the Computer Science subject area, and addressing topics related to post-quantum cryptography and IoT security, such as authentication, key exchange, digital signatures, architectures, frameworks, and reviews. This search resulted in 210 references from Scopus, 153 from IEEE Xplore, and 105 from Web of Science. The collected references were organized in Rayyan for preliminary screening of titles, keywords, and abstracts, followed by a manual thematic refinement process.

The final corpus comprised 30 peer-reviewed articles published between 2022 and 2026, which were selected using purposive thematic criteria. This selection prioritized studies that explicitly linked PQC with IoT environments, including the Industrial Internet of Things (IIoT), Internet of Medical Things (IoMT), edge computing, fog/cloud IoT, wireless IoT, and embedded systems. Additionally, the corpus included articles addressing pertinent security functions such as authentication, key exchange, digital signatures, access control, privacy-preserving computation, blockchain-based trust, protocol integration, and experimental evaluation on constrained platforms.

Each article underwent systematic organization through the use of a documentary extraction form that captured essential bibliographic data, identified the security focus, categorized the cryptographic algorithm, specified the IoT domain, noted the evaluation platform, and reported metrics, results, advantages, limitations, and future directions. Additionally, a complementary structured record of technical evidence was created, including key tables and figures that detailed performance, energy consumption, memory usage, latency, throughput, security levels, and implementation constraints. This

structured approach facilitated the cross-checking of incorporated information, thereby mitigating the risk of unsupported comparisons or unverified attributions.

The studies were organized according to the layered analytical architecture described in Section 3.3, and assigned to the layer that corresponded to their primary contribution. The analysis also addressed any cross-layer overlaps.

The corpus does not provide a comprehensive overview of PQC–IoT research. The deliberate selection criteria and restrictions regarding language, source, document type, and time period may have resulted in the exclusion of pertinent studies. Additionally, the variability in platforms, protocols, metrics, security levels, and experimental conditions hinders direct numerical comparison across studies. Consequently, this analysis predominantly employs a qualitative and comparative approach, with quantitative data presented only in the context of the studies that reported them.

3. CONCEPTUAL FRAMEWORK FOR POST-QUANTUM SECURITY IN LAYERED IOT SYSTEMS

3.1 Quantum Threat and Post-Quantum Cryptography

The advancement of quantum computing requires a reassessment of the security assumptions that underpin contemporary digital services. Two quantum algorithms are pivotal to understanding this threat model. Shor's algorithm poses a significant risk to classical public-key schemes that rely on integer factorization and discrete logarithms, including RSA, ECC, ECDSA, and Diffie–Hellman. Meanwhile, Grover's algorithm effectively reduces the security of symmetric encryption and hash functions by a quadratic factor, thereby necessitating larger key sizes to maintain equivalent security levels. These risks are further exacerbated by the "*harvest now, decrypt later*" scenario, in which encrypted data collected today may be decrypted in the future if sufficiently advanced quantum capabilities become available. This concern is particularly relevant for systems with extended operational lifespans, such as IoT deployments (Halak et al., 2024; Shim, 2024).

Post-quantum cryptography (PQC) encompasses public-key mechanisms that are grounded in mathematical problems for which no efficient quantum algorithms are currently known. Within the examined corpus, lattice-based mechanisms are prominent in key encapsulation mechanisms (KEMs), digital signatures, authentication, and access control. Notable examples include Kyber, Dilithium, Falcon, Falcon-M, NTRU, Rudraksh, and Ring-ExpLWE (Castiglione et al., 2025; Halak et al., 2024; Kerimbayeva et al., 2025; Kundu et al., 2025).

Other cryptographic families serve more specialized functions: hash-based signatures, such as SPHINCS+, XMSS, and LMS, are primarily employed in acceleration and embedded blockchain applications (Marchsreiter, 2025; Wu et al., 2025); code-based

mechanisms, including Classic McEliece, BIKE, and HQC find applications in hybrid Transport Layer Security (TLS) protocols and comparative KEM evaluations (Cruz-Piris et al., 2025; Zafar & Iqbal, 2025); and MPC-in-the-Head signatures are represented by AIMer as a non-lattice alternative (Kwon et al., 2025).

The corpus discusses multivariate and isogeny-based approaches primarily as comparative references rather than as leading evaluated options for IoT hardware. In particular, the treatment of SIKE reflects caution in light of recent cryptanalytic advances that have affected its security (Cruz-Piris et al., 2025; Shim, 2024). Hybrid approaches that combine post-quantum cyptography (PQC) with classical mechanisms, such as X25519 or AES, play a crucial role in ensuring interoperability during the migration process (Ojetunde et al., 2025; Zafar & Iqbal, 2025). While quantum key distribution (QKD) is recognized as a related quantum-security technology, it does not fall under the strict definition of PQC, as it relies on specific physical infrastructure rather than on post-quantum public-key primitives (Aneesh Kumar et al., 2025). Table 1 consolidates these various families of approaches.

Table 1

Cryptographic Families and Related Approaches Identified in the Corpus

Family or approach	Examples mentioned in the corpus	Main relevance for PQC-IoT
Lattice-based	Kyber, Dilithium, Falcon, Falcon-M, NTRU, Rudraksh, Ring-ExpLWE	KEMs, signatures, authentication, access control
Hash-based	SPHINCS+, XMSS, LMS	Signatures, blockchain, acceleration
Code-based	Classic McEliece, BIKE, HQC	Hybrid TLS, KEM comparison, migration
MPC-in-the-Head	AIMer	Non-lattice signature alternative
Multivariate	Rainbow	Comparative reference with cryptanalytic caution; limited role in the corpus
Isogeny-based	SIKE	Historical/comparative reference with cryptanalytic caution
Hybrid PQC + classical approaches	PQC with X25519, AES, or other classical mechanisms	Interoperability during migration
QKD	Quantum key distribution	Adjacent quantum-security technology; not PQC in the strict sense

Note. The table serves solely for conceptual orientation purposes. The summary of cryptographic families presented is intended as a conceptual overview, rather than a comparison of performance.

3.2 IoT Systems: Constraints, Attack Surfaces, and Traditional Architectural Models

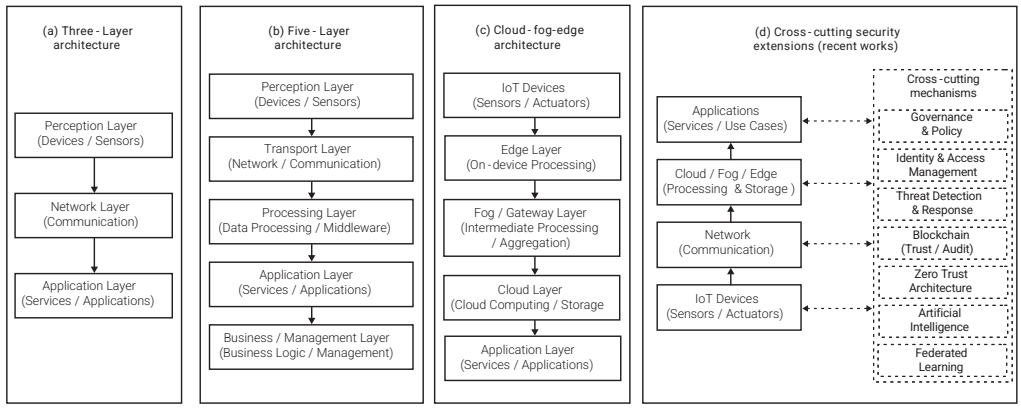
The adoption of PQC in the IoT differs from its implementation in general-purpose infrastructures due to the limitations faced by end nodes, which often operate with restricted RAM, flash memory, computational capacity, battery life, and bandwidth. These constraints

are particularly significant, as many PQC mechanisms use larger keys, ciphertexts, and signatures than classical schemes, and computational procedures that may impose considerable demands on constrained microcontrollers, sensors, and embedded devices (Halak et al., 2024; Kundu et al., 2025).

The limitations associated with IoT devices are exacerbated by their broad attack surface. These devices are often deployed in physically accessible environments and communicate over exposed or low-power channels. Consequently, they may encounter various types of attacks, including logical attacks such as man-in-the-middle, replay, and impersonation attacks, as well as physical attacks such as side-channel leakage (Marchsreiter, 2025; Shim, 2024). Therefore, the adoption of PQC in IoT must consider not only algorithmic security but also robustness of implementations and the context of deployment.

Figure 1

Classical Architectural Models of IoT and Contemporary Cross-Cutting Security Extensions



Note. The first three panels depict general architectural models for IoT, while the fourth panel demonstrates mechanisms such as blockchain, Zero Trust, artificial intelligence, federated learning, identity management, governance, and threat detection. These mechanisms operate across multiple layers rather than adhering to a single architectural level.

IoT systems have traditionally been represented through layered models. These include three-layer architectures focused on perception, network, and application functions; five-layer architectures that incorporate transport, processing, or business levels; and cloud–fog–edge models that efficiently distribute computation across devices, gateways, edge nodes, and cloud services. Recent studies have expanded these models by integrating cross-cutting mechanisms for governance, identity, threat detection, blockchain-based trust, Zero Trust architectures, artificial intelligence, and federated learning (Alatawi, 2025; Aleisa, 2025; Elkhodr, 2025). However, the original designs did not take into account post-quantum constraints, where concerns such as cryptographic overhead,

migration interoperability, and implementation security must now be prioritized. Figure 1 presents a summary of three general IoT architectural models along with one cross-cutting extension identified in the recent literature.

Consequently, the migration to PQC within IoT systems involves more than merely substituting vulnerable cryptographic primitives with quantum-resistant alternatives. The adoption of larger keys, ciphertexts, and signatures may lead to increased handshake size, latencies, and bandwidth consumption. Furthermore, the computational and memory overhead associated with these changes can influence whether operations are conducted locally or delegated to gateways or edge nodes. Additionally, existing legacy infrastructures require hybridization strategies during the migration process. These complexities underscore the need for an analytical framework that evaluates PQC approaches based on their functional impact on IoT systems, rather than viewing them solely as isolated algorithms (Cruz-Piris et al., 2025; Halak et al., 2024).

3.3 Layered Analytical Architecture for Organizing the Review

Drawing on these considerations, this review adopts a layered analytical architecture to systematically organize post-quantum security approaches for IoT. This architecture employs traditional IoT models as a foundational basis and reconfigures them to address the specific challenges posed by PQC, including constrained implementation, protocol migration, distributed trust, application-level requirements, privacy, and side-channel resistance. Rather than serving as a definitive taxonomy of the field, this framework aims to provide an interpretive lens for situating diverse contributions within a cohesive structure.

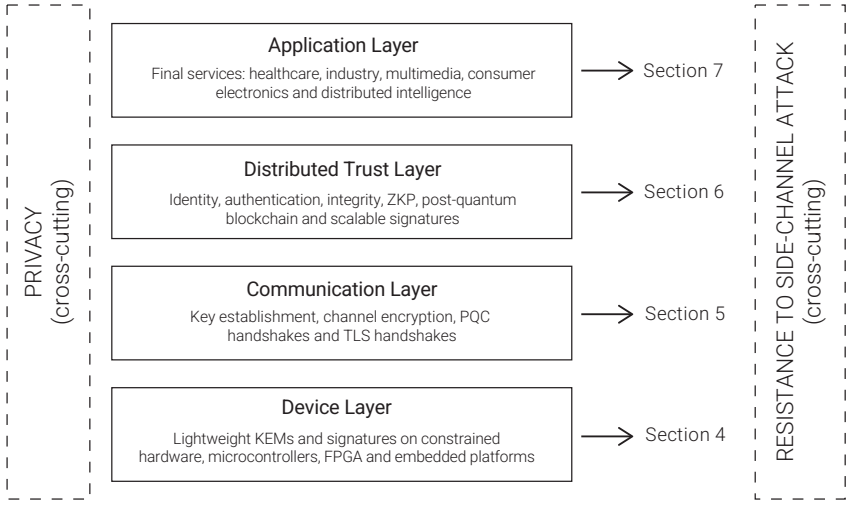
The architecture consists of four functional layers. The device layer encompasses end nodes and the local execution of PQC primitives on constrained hardware, where limitations in memory, energy, and computation are most pronounced. The communication layer facilitates secure data exchange among devices, gateways, edge nodes, and remote services, incorporating key establishment, channel encryption, transport protocols, and hybrid handshakes. The distributed trust layer incorporates mechanisms for identity, authentication, authorization, integrity, traceability, and decentralized verification, utilizing methods such as post-quantum blockchain, zero-knowledge proofs, access control, and scalable signatures. Finally, the application layer encompasses the IoT application domains that benefit from these security guarantees, including industrial, medical, wireless, multimedia, smart-grid, and AI-enabled environments.

Two cross-cutting dimensions enhance these layers. Privacy refers to guarantees that extend beyond channel confidentiality, including identity protection, privacy-preserving computation, federated learning, homomorphic encryption, differential privacy, and zero-knowledge mechanisms. Resistance to side-channel attacks pertains to the robustness of implementations against physical leakage, particularly in constrained

devices where cryptographic operations may be vulnerable to timing, power, electromagnetic, or fault-based analysis. These dimensions are categorized as cross-cutting because they influence multiple layers rather than being confined to a single system function. Figure 2 synthesizes the analytical architecture, illustrating the four functional layers alongside the two cross-cutting dimensions.

Figure 2

Layered Analytical Architecture for Organizing Post-Quantum Security Approaches in IoT Environments



Note. The four layers delineate the functional levels at which PQC affects IoT systems. Furthermore, privacy and resistance to side-channel attacks serve as cross-cutting dimensions within this framework. This model provides an overview to help readers compare and conceptualize the framework layers. It does not prescribe a deployment architecture.

This framework establishes the central organizing principle for the remainder of the review. Section 4 examines device-layer studies focused on lightweight Key Encapsulation Mechanisms (KEMs) and signatures tailored for constrained hardware. Section 5 analyzes communication-layer proposals that incorporate PQC stacks, protocols, and handshake processes. Section 6 engages in a discussion of distributed trust, authentication, blockchain, and mechanisms for perserving privacy. Section 7 provides a synthesis of research spanning various cryptographic families, application domains, and layers while also identifying exisiting research gaps. Finally, Section 8 delineates the conclusions drawn from this review.

4. DEVICE-LAYER APPROACHES: KEMS AND SIGNATURES ON CONSTRAINED HARDWARE

The device layer includes IoT end nodes and serves as the point where the costs associated with PQC become most evident. Low-end microcontrollers (MCUs), battery-powered sensors, embedded devices, and field-programmable gate arrays (FPGAs) operate within modest constraints of computational power, memory capacity, and energy consumption. In contrast, PQC primitives require larger key sizes, ciphertexts, and signatures compared to their classical counterparts. This corpus addresses the inherent tension by examining KEMs, digital signatures, and comparative evaluations conducted on embedded hardware.

Table 2 organizes the device-layer studies according to their contributions, platforms, and reported metrics. This table serves a descriptive purpose rather than a comparative one due to the heterogeneity of devices, implementations, and measurement settings. Figure 3 categorizes these studies into KEMs, digital signatures, and comparative evaluations.

Table 2

Assessment of Platforms and Metrics Reported in Studies within the Device Layer Corpus

Main contribution	Evaluated platform	Platform type	Reported metric categories	Studies
KEM (Rudraksh)	Virtex-7 and Artix-7 FPGA	FPGA	Area (LUT, FF, BRAM, DSP), latency (KG/Enc/Dec), frequency, time–area product	Kundu et al. (2025)
KEM (NTRU on Contiki-NG)	EFR32MG12 (Cortex-M4)	32-bit MCU	Cycles, stack, flash, power, energy, ciphertext size	Señor et al. (2022)
KEM (NTRUEncrypt)	Raspberry Pi 3B+ (Cortex-A53)	ARM Cortex-A SoC	Encryption and decryption times, key sizes, security levels	Al-Doori & Al-Gailani (2023)
KEM (Ring-ExpLWE)	Cortex-M0/M3 (software); Spartan-6 and Virtex-7 FPGA (hardware)	MCU + FPGA	Execution time, cycles, key and ciphertext sizes	Xu et al. (2022)
Signature (Falcon-M)	PC with Intel Core i7-9700K; Cortex-M4 and RISC-V as targets (not evaluated)	General-purpose PC; 32-bit MCU (target)	Key generation, signing, and verification times; RAM estimates	Kerimbayeva et al. (2025)
Signature (AIMer)	Cortex-M4 (Nucleo-L4R5ZI), Raspberry Pi 5, and MacBook Pro M4 (AArch64)	MCU + ARM SoC	KG/Sign/Verify cycles, stack, peak memory, code size, key and signature sizes	Kwon et al. (2025)

(*continues*)

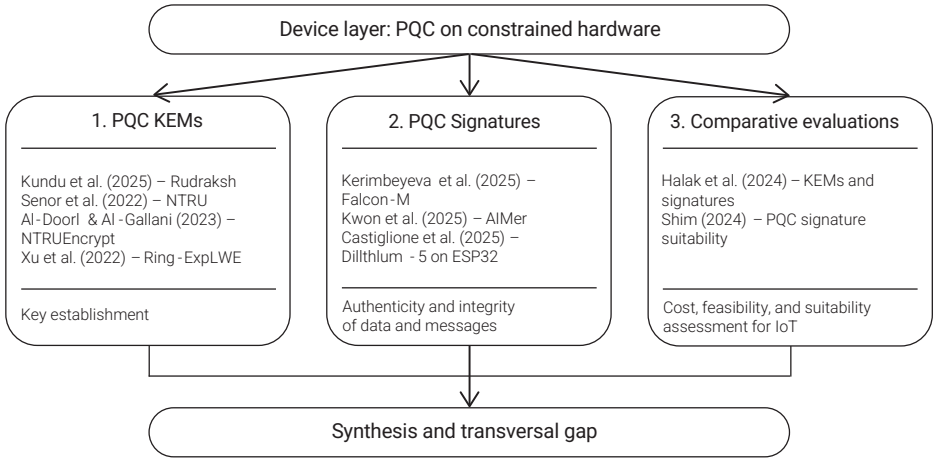
(*continued*)

Main contribution	Evaluated platform	Platform type	Reported metric categories	Studies
Signature (Dilithium-5)	ESP32 / ESP-WROOM-32D	Embedded platform with light-weight SoC	Key generation, signing, and verification times; key and signature sizes	Castiglione et al. (2025)
Comparative evaluation (KEMs and signatures)	STM32F469NI (Cortex-M4); RPi 3B+ and RPi Pico W as auxiliary nodes	32-bit MCU and ARM SoC	TLS/handshake latency, heap, stack, energy	Halak et al. (2024)
Review and comparative evaluation (PQC signatures)	Cortex-M3/M4, AArch64 (Cortex-A72, Apple M1), AVX2	Mixed platform	KG/Sign/Verify cycles, key and signature sizes, stack, energy; SCA (qualitative)	Shim (2024)

Note: SCA = side-channel attack.

Figure 3

Integration of PQC Approaches at the Device Layer



Note. The figure presents a consise overview of the analytical organization of device-layer studies categorized into KEMs, digital signatures, and comparative evaluations. It is not a performance ranking of the algorithms, authors, or platforms.

4.1 PQC KEMs for Constrained Hardware

The KEM studies employ three complementary strategies: designing compact mechanisms for lightweight hardware, implementing existing primitives on constrained platforms, and exploring algorithmic variants that are adapted for embedded execution.

Kundu et al. (2025) introduce Rudraksh, a compact MLWE-KEM designed specifically for lightweight hardware, which they evaluate on Virtex-7 and Artix-7 FPGAs. This design integrates lightweight modular arithmetic and employs ASCON-XOF as a pseudorandom function, while also conducting parameter exploration against Kyber and NewHope at NIST security level 1. The findings indicate that Rudraksh has a smaller area footprint compared to selected optimized references from Kyber.

Two studies assess the performance of NTRU-family mechanisms on ARM platforms. Señor et al. (2022) successfully integrate ntruhps2048509 into a Cortex-M4 microcontroller running Contiki-NG, optimizing it for IIoT-oriented WSNs and reporting metrics such as cycles, stack memory usage, flash requirements, power consumption, and energy usage. Concurrently, Al-Doori and Al-Gailani (2023) evaluate NTRUEncrypt on a Raspberry Pi 3B+ to facilitate edge/fog integration, providing insights into encryption and decryption times, as well as key sizes across different security levels. Collectively, these studies illustrate the application of the same cryptographic family within varied device-layer contexts and metric profiles.

Xu et al. (2022) introduce Ring-ExpLWE, a variant of Ring-LWE that employs a discrete exponential error distribution to enhance the security profile without incurring additional hardware costs. The authors evaluate this proposal using software implementations on Cortex-M0 and Cortex-M3, as well as through hardware evaluations on Spartan-6 and Virtex-7 FPGAs.

Overall, these studies affirm the feasibility of KEM at the device layer under controlled conditions; however, they identify a persistent limitation that remains to be addressed. This limitation pertains to the evaluation of side-channel attacks on actual hardware, which remains insufficient, as further discussed in Section 4.3.

4.2 PQC Signatures on Microcontrollers and Embedded Platforms

Digital signatures typically pose greater challenges than KEMs for constrained devices. This body of research identifies three strategies to mitigate this bottleneck: Falcon-M and Dilithium-5 within the lattice-based paradigm, and AIMer as an alternative based on the MPC-in-the-Head model.

Kerimbayeva et al. (2025) introduce Falcon-M, a lightweight variant of the Falcon signature scheme that employs random polynomials and FFT, intended to simplify key generation and reduce the memory footprint. While the targeted platforms include Cortex-M4 and RISC-V, the evaluation was conducted on an Intel Core i7-9700K, with preliminary RAM estimates indicating potential for embedded deployments. Consequently, this study provides an algorithmic profile that necessitates further validation on the intended hardware.

Kwon et al. (2025) optimize AIMer, a signature scheme utilizing the MPC-in-the-Head approach grounded in the AIM2 symmetric primitive. They evaluated their implementation on the Cortex-M4 and extended the analysis to AArch64 platforms, including Raspberry Pi 5 and Apple Silicon, reporting metrics such as cycles, stack usage, peak memory consumption, code size, and key/signature sizes. This AIMer work expands the discussion at the device-layer to incorporate analyses beyond lattice-based signatures.

Castiglione et al. (2025) integrate Dilithium-5 into an ESP32 microcontroller for a biomedical blockchain application. By employing PQClean and implementing polynomial optimizations via Kronecker substitution, the study reports that key generation, signing, and verification times range from tens to hundreds of milliseconds, contingent upon the specific configuration used.

Collectively, these studies indicate that the feasibility of signatures is heavily influenced by the choice of algorithmic family, implementation strategy, and platform. Dilithium-5 demonstrates successful deployment on commercially available, low-cost hardware, while Falcon-M highlights the benefits of algorithmic simplification, albeit with embedded validation still pending. Furthermore, AIMer broadens the design landscape beyond lattice-based signatures. Additionally, hash-based signatures such as SPHINCS+ are explored in various contexts, including acceleration and embedded blockchain applications.

4.3 Comparative Evaluations and Suitability Reviews for IoT

Halak et al. (2024) and Shim (2024) offer complementary comparative perspectives on PQC. Halak et al. (2024) evaluate PQC schemes on the STM32F469NI microcontroller, examining KEMs such as Kyber, Saber, and FrodoKEM, as well as signatures including Dilithium, Falcon, SPHINCS+, and SIKE. They also reference classical algorithms such as ECDHE/ECDSA with secp256r1 and AES-256. Their analysis includes metrics such as TLS and handshake latency, heap and stack memory consumption, and energy usage, revealing that lattice-based KEMs typically offer better performance than PQC signatures on constrained hardware.

In contrast, Shim (2024) focuses on PQC signatures for IoT devices, evaluating performance across Cortex-M3, Cortex-M4, AArch64, and AVX2 architectures. This study encompasses the schemes Dilithium, Falcon, SPHINCS+, and UOV, while also noting Rainbow —which has been compromised through algebraic and MinRank attacks (Kerimbayeva et al., 2025)— as well as XMSS, XMSSMT, and LMS in a broader comparative framework.

Together, these studies highlight a significant gap at the device layer. Although several PQC mechanisms can be implemented on constrained devices, experimental evaluations of side-channel leakage in real hardware are infrequently conducted. This gap is addressed further in Section 7.

5. APPROACHES AT THE COMMUNICATION LAYER: PQC STACKS, PROTOCOLS, AND HANDSHAKES

The communication layer facilitates secure data exchange among devices, gateways, and remote services, encompassing key establishment, channel encryption, transport protocols, and legacy stacks. PQC impacts this layer by increasing handshake size, latency, and bandwidth consumption due to the utilization of larger keys, ciphertexts, and signatures. This corpus examines the resulting challenges from three perspectives: the integration of PQC within the existing TLS protocol, the deployment of PQC through ad-hoc combinations of KEM, signatures, and lightweight authenticated encryption over wireless and low-power wide-area networks (LPWAN), and the incorporation of PQC within legacy industrial protocols.

Table 3 categorizes the six communication-layer studies based on protocol or stack, security mechanisms, evaluation environments, and reported metrics. Consistent with the previous section, this table serves a descriptive purpose and should not be interpreted as a direct numerical comparison across diverse networks, platforms, and experimental conditions.

Table 3

Protocols, Security Mechanisms, and Documented Metrics within the Communication Layer

Protocol or stack	Security algorithms and mechanisms used	Evaluation environment	Reported metric categories	Studies
KEMTLS in IIoT	KEMs: BIKE, Kyber, FrodoKEM, HQC; signatures: Dilithium, Falcon, SPHINCS+, HAWK	Raspberry Pi 2 and 3 (IIoT scenarios)	TLS/handshake latency, energy, KG/Enc/Dec and signature times	Cruz-Piris et al. (2025)
Hybrid TLS 1.3 (PQC + classical)	Classic McEliece, BIKE, Kyber; X25519, RSA/ECC; QRNG, MFA	Intel Core i7-9700K PC; emulated IoT scenarios	Handshake latency, CPU, memory, throughput, QRNG entropy	Zafar & Iqbal (2025)
Lightweight PQC stack over NB-IoT (CoAP)	Kyber-768, SPHINCS+-128f, ChaCha20-Poly1305	ESP32-WROOM-32 + SIM7080G	Per-layer latency, current, peak RAM, firmware size	Do & Tran (2026)
IEEE 802.11n; PQC standalone and PQC-AES modes	Kyber, BIKE, HQC; Falcon; AES-256; HMAC-SHA256; HKDF	Client–server over IEEE 802.11n	KEM times, signature times, latency, throughput	Ojetunde et al. (2025)
Hybrid KEM + authenticated encryption framework	Kyber-512 + ASCON	Controlled testbed, 50 runs	Encryption time, RAM, CPU, energy, entropy	Mahdi & Abdullah (2025)

(*continues*)

(*continued*)

Protocol or stack	Security algorithms and mechanisms used	Evaluation environment	Reported metric categories	Studies
Post-SECS/GEM (PQC extension)	Kyber + Dilithium + AES-GCM-256 + HMAC-SHA3	Raspberry Pi 4; Ethernet; emulated network	Encryption/decryption, signing/verification, and key establishment. Evaluation metrics: CPU usage, memory consumption, and energy consumption	Al-Mekhlafi et al. (2026)

Note. This table provides a descriptive overview and does not constitute a direct performance comparison across diverse protocols, networks, and platforms. The following acronyms are defined for clarity: NB-IoT = narrowband IoT; CoAP = Constrained Application Protocol; KEMTLS = key-encapsulation-mechanism TLS; QRNG = quantum random number generator; MFA = multi-factor authentication; HKDF = HMAC-based key derivation function.

5.1 PQC in TLS and Transport Handshakes

Two studies examine post-quantum migration in TLS using complementary strategies: restructuring the handshake process and maintaining hybrid interoperability with classical infrastructure.

Cruz-Piris et al. (2025) evaluate PQC in IIoT by implementing KEMTLS on Raspberry Pi 2 and 3. Their analysis includes various KEMs such as BIKE, Kyber/ML-KEM, FrodoKEM, and HQC, along with digital signatures like Dilithium/ML-DSA, Falcon, SPHINCS+, and HAWK. Their findings indicate that KEMTLS handshakes introduce overhead when compared to classical TLS. Zafar and Iqbal (2025) prioritize interoperability by integrating Classic McEliece and BIKE with X25519, RSA/ECC, QRNG, and MFA within a hybrid TLS 1.3 framework designed for gradual migration.

Collectively, these studies demonstrate that post-quantum transport migration involves more than mere primitive selection; it necessitates deliberate protocol-level decisions regarding handshake structure, hybrid coexistence, and integration with legacy systems.

5.2 PQC in Wireless Networks, LPWAN, and IoT Channels

Three studies in the corpus present initial evidence for deploying PQC stacks in standard wireless networks, LPWAN channels, and generic IoT communications.

In their 2026 study, Do and Tran propose a lightweight hybrid stack for NB-IoT that integrates CRYSTALS-Kyber-768, SPHINCS+-SHA256-128f, and ChaCha20-Poly1305 on the ESP32-WROOM-32 platform using the SIM7080G and CoAP. This approach utilizes session persistence and buffer reuse strategies to mitigate the costs associated with handshakes.

Ojetunde et al. (2025) implement secure IEEE 802.11n communication modes, including standalone PQC and hybrid PQC-AES. They evaluate various algorithms, including Kyber/ML-KEM, BIKE, HQC, Falcon/FN-DSA, AES-256, and HMAC-SHA256. Their findings indicate that lattice-based KEMs show lower execution times compared to BIKE and HQC, and that hybrid PQC-AES configurations become increasingly advantageous as the volume of transmitted data increases.

Mahdi and Abdullah (2025) combine Kyber-512 and ASCON within a controlled testbed, reporting reductions in time, memory usage, CPU consumption, and energy expenditure compared to a configuration that relies solely on Kyber, all while maintaining near-maximum entropy.

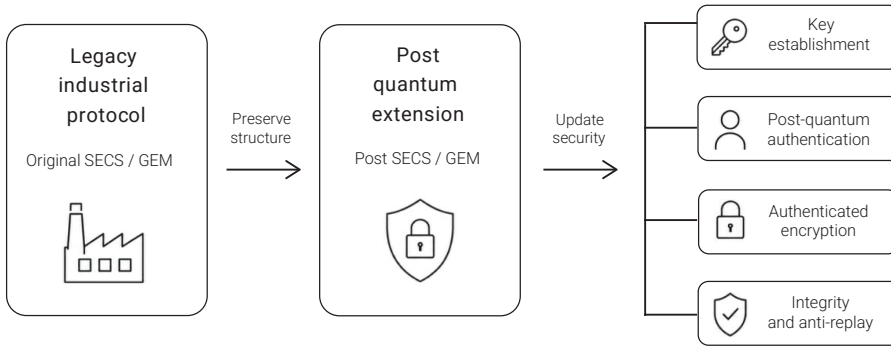
These studies indicate that lattice-based KEMs, when combined with lightweight authenticated encryption, represent a practical solution for constrained channels. In contexts such as Narrowband Internet of Things and broader wireless networks, where session persistence, reuse and compactness are critical, this approach effectively addresses the issue of repeated PQC handshakes that can significantly increase communication costs.

5.3 PQC in Legacy Industrial Protocols

Legacy industrial protocols require the development of migration strategies that enhance security without compromising operational behavior. This corpus addresses this challenge through a specific contribution centered on SECS/GEM in industrial automation.

Figure 4

Adaptation of Legacy Industrial Protocols to the Post-Quantum Paradigm



Note. The figure illustrates the adaptation of an established industrial protocol via a post-quantum extension, which maintains the integrity of the operational structure while enhancing security mechanisms.

Al-Mekhlafi et al. (2026) introduce Post-SECS/GEM, a post-quantum extension that integrates CRYSTALS-Kyber for encapsulation and session-key derivation,

CRYSTALS-Dilithium for authentication, AES-GCM-256 for authenticated encryption, and HMAC-SHA3 for integrity. The evaluation of this framework was conducted on a Raspberry Pi 4 under switched Ethernet and emulated network conditions. The framework effectively combines authentication, confidentiality, integrity, and safeguards against replay and DoS attacks while maintaining the operational structure of SECS/GEM. Figure 4 illustrates this adaptation logic.

This case underscores the necessity of coexistence with legacy infrastructure. In the context of industrial IoT, the migration to PQC typically involves enhancing security protocols rather than replacing them entirely.

6. DISTRIBUTED TRUST, AUTHENTICATION, AND POST-QUANTUM PRIVACY

This section analyzes 14 studies on distributed trust, authentication, and post-quantum privacy. Unlike investigations focused solely on the device and communication layers, this discussion encompasses not only algorithm execution and transport protocols but also mechanisms that uphold identity, authorization, traceability, verification, and privacy at the system level. The studies are characterized into three main themes: authentication and access control; blockchain, scalable signatures, and acceleration; and integrated frameworks for trust and operational privacy.

Table 4 summarizes these studies, detailing their focus, mechanisms, domain, type of contribution, and supporting evidence. This table serves as a navigational tool rather than a direct comparison among proposals that differ in objectives, platforms, and validation methodologies.

Table 4

Methodological Approaches, Mechanisms, and Forms of Contribution in Research Pertaining to the Distributed Trust, Authentication, and Privacy Layer

Focus	Mechanisms and technologies used	Domain	Contribution	Studies
PAKE	LWE (MP-SPHF)	General IoT	Algorithmic analysis	Li & Wang (2022)
Three-party mutual authentication	RLWE	IIoT	Protocol with simulation	Kim et al. (2026)
Three-factor authentication	RLWE + fuzzy extractor	IoMT	Protocol with evaluation	Ahmad et al. (2026)
Access control	RLWE-CP-ABE + Dilithium + AES-GCM	Cloud IoT, healthcare	Experimental evaluation	Poomekum et al. (2025)

(*continues*)

(*continued*)

Focus	Mechanisms and technologies used	Domain	Contribution	Studies
Scalable signatures	Fractional Verkle Trees (FVDS)	Blockchain, IoT firmware	PC-based prototype	Iavich et al. (2025)
Post-quantum blockchain	Dilithium, Falcon, SPHINCS+, XMSS-MT + PKR	IoT, energy, vehicular	Evaluation on embedded devices	Marchsreiter (2025)
Signature acceleration	SPHINCS+ + GPU batching	Cloud IoT, AIoT	GPU benchmarks	Wu et al. (2025)
Signature acceleration	HAETAE + GPU kernel fusion	IIoT, edge/cloud	GPU benchmarks	Wu et al. (2026)
Authentication with ZKP	Schnorr-ZKP + HE + blockchain	General IoT	Simulation	Tawfik et al. (2025)
ZTA + blockchain + ZKP	DQN + blockchain + ZKP	General IoT	Dataset-based simulation	Aleisa (2025)
AI + blockchain + PQC framework	Q-learning + blockchain + hybrid encryption + FL + DT	General IoT	Simulation	Elkhodr (2025)
6G edge + FL + blockchain	CNN-LSTM + Hyperledger + Kyber + Dilithium	Industry 5.0, smart grid	Edge-based evaluation	Alatawi (2025)
Privacy-preserving FL	FedAvg + GRU + HE + DP	IoT networks	Simulation with CICIDS2017	Rahmati & Pagano (2025)
Private inference	PDTE + SWHE (RLWE)	IIoT, healthcare	PC-based evaluation	Kjamilji (2024)

Note. This table provides a descriptive overview and should not be interpreted as a direct comparison of proposals that pursue varying objectives. The following acronyms are defined for clarity: ZKP = zero-knowledge proof; ZTA = Zero Trust architecture; FL = federated learning; HE = homomorphic encryption; DP = differential privacy; PKR = public-key recovery; DQN = deep Q-network; SWHE = somewhat homomorphic encryption; DT = digital twin; CNN = convolutional neural network; LSTM = long short-term memory; GRU = gated recurrent unit.

6.1 Post-Quantum Authentication, Key Management, and Access Control

Four studies contribute to advancing post-quantum authentication, key agreement, and access control mechanisms. Li and Wang (2022) propose a one-round lattice-based PAKE protocol that utilizes the MP-SPHF framework, effectively reducing communication costs for constrained nodes, although the evaluation remains purely analytical. Kim et al. (2026) develop a robust three-party RLWE-based mutual authentication protocol tailored for IIoT, complemented by a comprehensive security analysis and NS-3 simulations. Ahmad et al. (2026) integrate biometrics, passwords, and smart card factors within the RLWE framework for IoMT, employ a fuzzy extractor to mitigate biometric noise, and present results on computational efficiency, communication overhead, and scalability. Poomekum et al. (2025) broaden the discussion of fine-grained access control by employing RLWE-CP-ABE,

Dilithium-2, AES-256-GCM, attribute-hash revocation, salts, epoch-based blacklists, and fog computing assistance to alleviate the burden on end nodes.

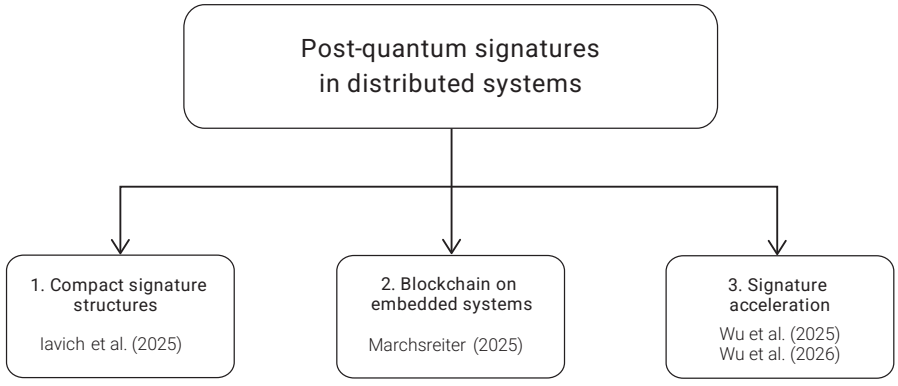
These proposals, while sharing a foundational lattice/RLWE structure, address distinct trust relationships—including password-authenticated key exchange, three-party mutual authentication, multifactor authentication, and attribute-based access control. Consequently, the migration to PQC at this layer is best interpreted as a diverse repertoire of mechanisms tailored to various trust models rather than a singular primitive approach.

6.2 Post-Quantum Signatures for Blockchain, Traceability, and Scalable Processing

In distributed systems such as blockchain, trust is primarily established through signatures that verify records, transactions, firmware updates, or identities. In the context of post-quantum systems, signature size, verification costs, and aggregate processing volume may pose limitations across the entire IoT stack, ranging from constrained end devices to gateways, edge nodes, and cloud services. The research discussed in this subsection addresses these challenges by developing compact signature structures, deploying embedded blockchain solutions, and implementing acceleration techniques for high-volume verification. Figure 5 provides a summary of these three strategies.

Figure 5

Emerging Research Trends in Post-Quantum Signatures for Distributed Systems



Note. This figure categorizes the studies in this subsection based on their primary area of focus, which includes compact signature structures, blockchain applications in embedded systems, and signature acceleration. It is important to clarify that the figure does not serve as a performance comparison among the various proposals presented.

Iavich et al. (2025) propose Fractional Verkle Trees and FVDS as a compact alternative to post-quantum Merkle-tree approaches for scenarios involving numerous signers. Their evaluation is conducted through a Python prototype on a personal computer. Marchsreiter

(2025) assesses post-quantum blockchain signatures on embedded systems, examining variants such as Dilithium, Falcon, SPHINCS+, and XMSS-MT. Additionally, he introduces public-key recovery to reduce on-chain credential storage, utilizing experiments on an Intel Core i7 and a Raspberry Pi 3B. Wu et al. (2025) enhance the performance of SPHINCS+ by implementing CUDA-based intra-block batch processing on RTX GPUs. Furthermore, Wu et al. (2026) optimize HAETAE on the Jetson Xavier and RTX 4090 through techniques such as kernel fusion and coarse-grained parallelism. These studies on acceleration are particularly significant for gateways, edge nodes, and cloud services that handle large volumes of signatures.

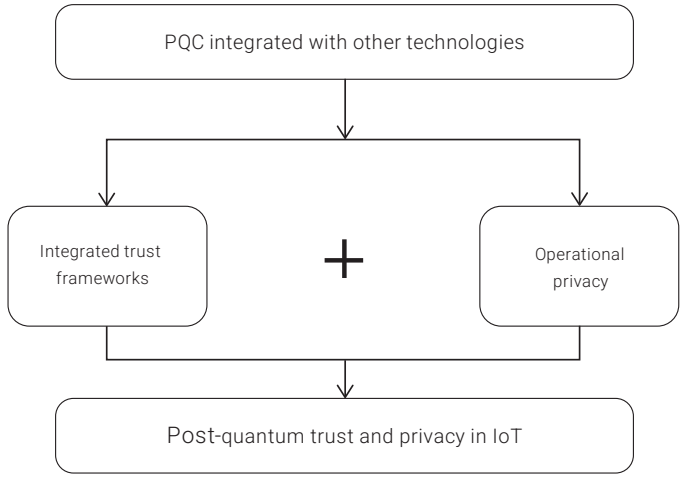
Collectively, these research efforts demonstrate that achieving post-quantum integrity and traceability in distributed IoT systems necessitates a focus on compactness, the feasibility of embedded systems, and the capacity for high-throughput verification.

6.3 Integrated Frameworks for Post-Quantum Trust and Operational Privacy

Six studies examine PQC as an integral component of broader architectures rather than as an isolated primitive. These studies can be divided into two complementary groups: integrated trust frameworks, which combine blockchain, ZKP, Zero Trust, AI, or federated learning to facilitate system-level coordination; and operational privacy mechanisms that safeguard data during training, detection, or inference. Figure 6 illustrates this relationship.

Figure 6

Exploring the Relationship between Integrated Trust Frameworks and Operational Privacy



Note: This figure delineates integrated trust frameworks from operational privacy. Integrated trust frameworks are designed to coordinate security at the system level, whereas operational privacy focuses on protecting data during training, detection, or inference. Both approaches are conceptualized as complementary rather than mutually exclusive categories.

Tawfik et al. (2025) integrate Schnorr-type zero-knowledge proofs over Module-SIS framework with homomorphic encryption and blockchain technologies to facilitate traceable and privacy-preserving authentication. Aleisa (2025) introduces QBC-ZKPAF, a Zero Trust architecture that combines ZKP, blockchain, and reinforcement learning, and evaluates it on the Edge-IIoTset. Elkhodr (2025) presents IASF-IoT, which orchestrates artificial intelligence, blockchain, post-quantum hybrid encryption, digital twins, and federated learning through a Q-learning-based security orchestrator across more than 1,000 simulated heterogeneous devices. Alatawi (2025) employs a similar convergence to Industry 5.0 by developing EdgeGuard-IoT, which integrates secure federated learning, Hyperledger Fabric, Kyber, Dilithium, and Zero Trust authentication on Raspberry Pi 4 and Jetson Nano edge nodes. While these frameworks share a compositional logic, they differ in their respective domain, evaluation methodologies, and the realism of their deployment scenarios.

Operational privacy is illustrated through the findings of two studies. Rahmati and Pagano (2025) integrate federated learning, homomorphic encryption, and differential privacy for IoT threat detection, utilizing the CICIDS2017 dataset in conjunction with a GRU model. Their research reports enhanced detection metrics and a reduction in membership inference success. In another study, Kjamilji (2024) introduces the PDTE scheme, which is based on the Ring-LWE approach and operates under the decision-RLWE model. This scheme is evaluated on benchmarks in healthcare, spam detection, and image recognition, using an Intel Core i9 processor.

Overall, the corpus indicates that achieving post-quantum privacy relies on the composition of multiple primatives rather than on a single primitive. However, the transferability across different domains and the behavior in large-scale production deployments remain insufficiently documented.

7. COMPARATIVE SYNTHESIS, APPLICATION DOMAINS, AND RESEARCH AGENDA

This section synthesizes the findings from various cryptographic families, application domains, and layered architectures, and identifies research gaps based on the studies analyzed in Sections 4 to 6.

7.1 Cryptographic Families Present in the Corpus

The corpus clearly demonstrates the predominance of lattice-based mechanisms, which serve multiple functions. These mechanisms are integral to KEMs such as Kyber and NTRU, digital signatures including Dilithium and Falcon, authentication protocols such as RLWE, and access control systems such as RLWE-CP-ABE.

Hash-based mechanisms are represented by SPHINCS+, XMSS-MT, and LMS within communication stacks, scalable signatures, acceleration, and blockchain applications.

Code-based mechanisms are exemplified by Classic McEliece and BIKE in hybrid TLS, along with HQC in comparative evaluations. Additionally, MPC-in-the-Head signatures manifest through AIMer across various platforms. Multivariate and isogeny-based families remain marginal, primarily serving as comparative references, while SIKE is approached with caution due to its documented cryptanalytic vulnerabilities. QKD is included as an adjacent technology in one multimedia encryption proposal; however, it is not treated as PQC in the strictest sense. Table 5 consolidates this distribution.

Table 5

Cryptographic Families identified in the Corpus

Family	Base problem	Algorithms in the corpus	Relative maturity in the corpus
Lattice-based	LWE, RLWE, NTRU, MLWE, SIS	Kyber, Dilithium, Falcon, Falcon-M, NTRU, Rudraksh, Ring-ExpLWE, MP-SPHF, RLWE-CP-ABE, HAETAE	Dominant; covers KEMs, signatures, authentication, and access control
Hash-based	Resistance of hash functions	SPHINCS+, XMSS-MT, LMS	Consolidated; present in scalable signatures and blockchain
Code-based	Decoding of linear codes	Classic McEliece, BIKE, HQC	Limited presence; present in hybrid TLS and comparative evaluations
MPC-in-the-Head	Multiparty computation over symmetric primitives	AIMer	Emerging; one evaluated proposal in the corpus
Multivariate	Nonlinear systems over finite fields	Rainbow, broken via cryptanalytic attacks, and other multivariate schemes	Marginal; comparative reference only
Isogeny-based	Isogenies between supersingular curves	SIKE, with warning due to cryptanalytic break	Limited presence; appears with warning due to cryptanalytic break
Complementary quantum cryptography	Quantum principles	QKD	Adjacent; not PQC in the strict sense

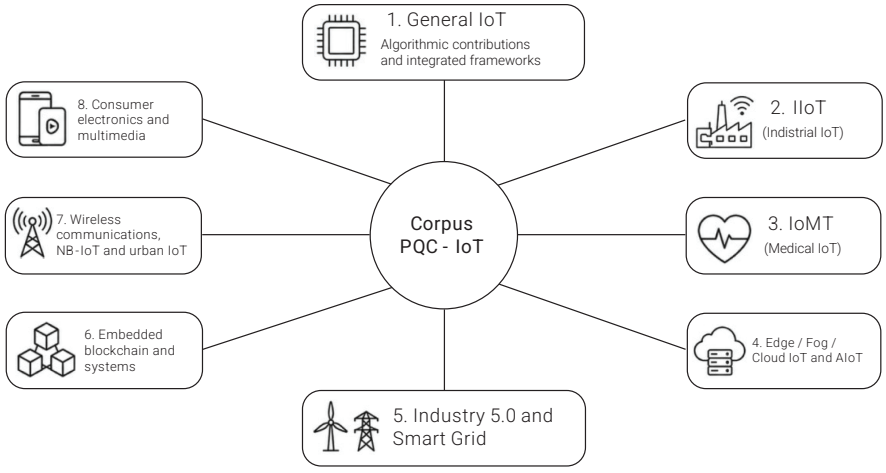
Note: This table provides a comprehensive summary of the families and associated categories identified within the corpus. It is important to note that hybrid combinations are excluded from classification as an independent family, as the integration of PQC + classical hybridization is considered a transitional strategy.

7.2 IoT Application Domains in the Corpus

The corpus encompasses various IoT domains, though their representation is not uniform. Figure 7 illustrates these areas for orientation purposes.

Figure 7

Identification of IoT Application Domains within the Corpus



Note: The figure provides a summary of the application domains identified within the corpus. It is important to note that the positioning of these domains does not reflect precise quantitative prevalence, as multiple studies may contribute to more than one domain.

The domain of the IoT encompasses both algorithmic advancements and comprehensive integrated frameworks. Notable contributions include PAKE and lattice-based authentication (Li & Wang, 2022), KEMs along with algorithmic variants designed for constrained hardware (Kundu et al., 2025; Xu et al., 2022), and signatures optimized for deployment on constrained platforms (Castiglione et al., 2025; Kerimbayeva et al., 2025; Kwon et al., 2025). Furthermore, suitability evaluations conducted on embedded platforms are reported (Halak et al., 2024; Shim, 2024), alongside integrated frameworks leveraging blockchain technomoby, ZKP, the Zero Trust model, and artificial intelligence (Aleisa, 2025; Elkhodr, 2025; Tawfik et al., 2025).

The Industrial Internet of Things (IIoT) serves as another critical area of focus, which including WSNs tailored for industrial settings (Señor et al., 2022), implementations of three-party mutual authentication (Kim et al., 2026), evaluations of KEMTLS (Cruz-Piris et al., 2025), private inference techniques (Kjamilji, 2024), GPU acceleration for enhanced aggregate processing (Wu et al., 2026), and the migration of legacy industrial protocols (Al-Mekhlafi et al., 2026).

IoMT manifests more specifically in the context of RLWE-based multifactor authentication (Ahmad et al., 2026) and healthcare components integrated into broader access-control or private-inference frameworks (Kjamilji, 2024; Poomekum et al., 2025).

Furthermore, the domains of edge, fog, cloud IoT, and AIoT encompass various technologies, including NTRU on ARM within edge and fog environments (Al-Doori & Al-Gailani, 2023), fog-assisted access control (Poomekum et al., 2025), GPU acceleration for signature processing in cloud and edge contexts (J. Wu et al., 2025; W. Wu et al., 2026), and the application of federated learning for threat detection (Rahmati & Pagano, 2025).

More specific applications arise in Industry 5.0 and smart grid systems, supported by a 6G-enabled edge intelligence framework (Alatawi, 2025). Additionally, developments in embedded blockchain technology focus on scalable signatures and public-key recovery (Iavich et al., 2025; Marchsreiter, 2025). In the realm of wireless communications and NB-IoT, IEEE 802.11n and LPWAN proposals offer innovative solutions (Do & Tran, 2026; Ojetunde et al., 2025). Finally, advancements in consumer electronics and multimedia are represented by an image-encryption proposal that integrates NTRU, QKD, and Falcon (Aneesh Kumar et al., 2025).

Two patterns emerge from this analysis. First, several studies contribute to multiple domains, indicating that the primary assignments listed in Supplementary Material S1 should not be considered exclusive. Second, the density of domainsrepresented in this corpus reflects specific contributions rather than the overall prevalence in the field. Areas such as smart homes, critical infrastructure, and the metaverse are underrepresented in this corpus, though they are not necessarily absent from the broader research landscape of PQC in the IoT.

7.3 Mapping the Corpus onto the Layered Analytical Architecture

The layered analytical architecture presented in Section 3 situates each study according to its primary contribution. Table 6 summarizes this mapping across the device, communication, distributed trust, and application layers.

Table 6

Mapping the Corpus onto the Layered Analytical Architecture

Layer or dimension	Key functions	Studies
Device layer	Lightweight KEMs and signatures on constrained hardware	Al-Doori & Al-Gailani (2023); Castiglione et al. (2025); Halak et al. (2024); Kerimbayeva et al. (2025); Kundu et al. (2025); Kwon et al. (2025); Señor et al. (2022); Shim (2024); Xu et al. (2022)
Communication layer	Key establishment, channel encryption, PQC stacks, and handshakes	Al-Mekhlafi et al. (2026); Cruz-Piris et al. (2025); Do & Tran (2026); Mahdi & Abdullah (2025); Ojetunde et al. (2025); Zafar & Iqbal (2025)

(*continues*)

(*continued*)

Layer or dimension	Key functions	Studies
Distributed trust layer	Authentication, identity, integrity, blockchain, ZKP, scalable signatures, and operational privacy	Ahmad et al. (2026); Alatawi (2025); Aleisa (2025); Elkhodr (2025); Iavich et al. (2025); Kim et al. (2026); Kjamilji (2024); Li & Wang (2022); Marchsreiter (2025); Poomekum et al. (2025); Rahmati & Pagano (2025); Tawfik et al. (2025); Wu et al. (2025); Wu et al. (2026)
Application layer	Final services built on the guarantees provided by the previous layers	Aneesh Kumar et al. (2025)
Privacy (cross-cutting)	Guarantees beyond channel confidentiality	Aleisa (2025); Elkhodr (2025); Kjamilji (2024); Poomekum et al. (2025); Rahmati & Pagano (2025); Tawfik et al. (2025)
Resistance to side-channel attacks (cross-cutting)	Robustness against physical leakage	Identified as a gap by Halak et al. (2024); Kerimbayeva et al. (2025); Kundu et al. (2025); Marchsreiter (2025); Señor et al. (2022); and Shim (2024).

This mapping supports two key observations. First, the device and communication layers present the most detailed algorithmic and experimental evidence, aligning with their identification as significant bottlenecks in the migration to PQC. Second, the distributed trust layer encompasses the most comprehensive array of integrated mechanisms, which underscores the systemic importance of identity, integrity, traceability, and privacy within the IoT.

Several studies exhibit intersections across these layers. For instance, Castiglione et al. (2025) establish a connection between the device and distributed trust layers by implementing Dilithium-5 on ESP32 within a blockchain use case. Al-Mekhlafi et al. (2026) link the communication and distributed trust layers by combining Kyber, Dilithium, and AES-GCM in SECS/GEM. Additionally, Alatawi (2025) bridges the distributed trust and application domains through the use of EdgeGuard-IoT for Industry 5.0. Table 6 categorizes each study according to its primary contribution, while discussions of overlaps occur in the relevant sections.

The cross-cutting dimensions exhibit distinct behaviors. Privacy emerges as a significant operational contribution across six studies, primarily through techniques such as federated learning, homomorphic encryption, differential privacy, ZKP, blockchain, and access control. In contrast, resistance to side-channel attacks is predominantly presented as an open limitation rather than as an evaluated property. This asymmetry represents one of the most notable gaps within the existing literature.

7.4 Common Gaps and Research Agenda

The cross-sectional analysis identifies three recurring gaps. The first and most prominent gap is the insufficient experimental evaluation of side-channel resistance on actual hardware. While several studies demonstrate the feasibility of PQC on constrained platforms, the resistance to physical leakage is largely presented as a limitation or future research direction across KEMs, digital signatures, and post-quantum blockchain implementations (Halak et al., 2024; Kerimbayeva et al., 2025; Kundu et al., 2025; Marchsreiter, 2025; Señor et al., 2022; Shim, 2024).

The second gap concerns sustained migration within real IoT ecosystems. Most evaluations predominantly depend on simulations, controlled testbeds, laboratory platforms, or emulated scenarios. As a result, evidence regarding longitudinal deployment costs, system stability, maintenance needs, hardware upgrades, interoperability with heterogeneous networks, and overall total cost of ownership remains limited. Furthermore, the technical metrics reported, such as latency, energy consumption, memory capacity, throughput, key size, and signature size, are seldom linked to sector-specific deployment decisions.

The third gap pertains to the transferability of integrated frameworks that combine PQC with federated learning, homomorphic encryption, differential privacy, zero-knowledge proofs, blockchain, or artificial intelligence. Current evaluations are often constrained to specific datasets, simulations, or platforms, raising unresolved questions regarding the behavior of these frameworks in large-scale production environments and their generalizability across different domains (Aleisa, 2025; Kjamilji, 2024; Rahmati & Pagano, 2025; Tawfik et al., 2025). Furthermore, this limitation is exacerbated by inconsistent reporting of standardization status by NIST, as well as by variations in security levels and comparisons with AES-equivalent security.

The resulting agenda is threefold: first, evaluating PQC against side-channel attacks on real hardware; second, studying longitudinal migrations while considering operational costs and critical sectors; and third, validating composite trust and privacy frameworks in production environments. Future reviews should aim to expand the corpus to include underrepresented families, platforms, and network technologies.

8. CONCLUSIONS

This narrative review demonstrates that the migration to PQC in the IoT entails more than merely replacing vulnerable asymmetric primitives. It significantly impacts constrained hardware, communication protocols, identity and authentication processes, privacy-preserving measures, and application services. Consequently, these transitions should be understood as a systemic transformation of IoT security.

The reviewed research articles predominantly feature lattice-based mechanisms, while hash-based, code-based, and MPC-in-the-Head families serve complementary roles. The exploration of hybrid approaches and compositions involving blockchain, zero-knowledge proofs, federated learning, homomorphic encryption, AI, and Zero Trust demonstrates that achieving post-quantum security in IoT relies on tailored combinations suited to specific functional layers and application domains.

The most significant gaps persist in the limited validation of side-channel resistance on actual hardware, the scarcity of longitudinal migration studies, the weak correlation between technical metrics and operational deployment costs, and the inadequate validation of integrated trust and privacy frameworks within large-scale heterogeneous environments.

This review contributes to the organization of a heterogeneous field by implementing a layered analytical architecture, identifying recurrent patterns within the included studies, and delineating existing research gaps. It is important to interpret these conclusions within the context of a narrative, non-exhaustive corpus, rather than as a comprehensive coverage of the PQC-IoT field.

Data Availability Statement

The comprehensive characterization matrix of the 30-study corpus can be accessed as Supplementary Material S1 at the following link: https://docs.google.com/spreadsheets/d/18fGUvDLxUFv6TFWoEqILFE75plqhGSZjstl_Fmk_304

REFERENCES

Ahmad, A., Jagatheswari, S., & Praveen, R. (2026). Quantum-secure lightweight fuzzy extractor based user authentication scheme for Internet of Medical Things. *Soft Computing, 30*, 787-808. https://doi.org/10.1007/s00500-025-11021-z

Alatawi, M. N. (2025). EdgeGuard-IoT: 6G-enabled edge intelligence for secure federated learning and adaptive anomaly detection in Industry 5.0. *Computers, Materials & Continua, 85*(1), 695-727. https://doi.org/10.32604/cmc.2025.066606

Al-Doori, M. J., & Al-Gailani, M. F. (2023). Securing IoT networks with NTRU cryptosystem: A practical approach on ARM-based devices for edge and fog layer integration. *International Journal of Intelligent Engineering & Systems, 16*(5), 462-472. https://doi.org/10.22266/ijies2023.1031.40

Aleisa, M. A. (2025). Blockchain-enabled zero trust architecture for privacy-preserving cybersecurity in IoT environments. *IEEE Access, 13*, 18660-18676. https://doi.org/10.1109/ACCESS.2025.3529309

Al-Mekhlafi, Z. G., Altmemi, J. M. H., Al-Shareeda, M. A., Al-Al-Hchaimi, A. A. J., Gaber, T., Homod, R. Z., Mohammed, B. A., Alshammari, G., Al-Dhlan, K. A., Alrashdi, R., & Alkhabra, Y. A. (2026). A post-quantum secure solution for SECS/GEM communications in Industrial Internet of Things (IIoT) application. *IEEE Open Journal of the Communications Society, 7*, 670-684. https://doi.org/10.1109/OJCOMS.2026.3654010

Aneesh Kumar, K. B., Mohith, L. S., Jain, K., Krishnan, P., Venkatachalam, N., & Buyya, R. (2025). Post-quantum cryptography-based multimedia encryption communication scheme in IoT consumer electronics. *IEEE Transactions on Consumer Electronics*, *71*(2), 4995-5006. https://doi.org/10.1109/TCE.2025.3572949

Castiglione, A., Esposito, J. G., Loia, V., Nappi, M., Pero, C., & Polsinelli, M. (2025). Integrating post-quantum cryptography and blockchain to secure low-cost IoT devices. *IEEE Transactions on Industrial Informatics, 21*(2), 1674-1683. https://doi.org/10.1109/TII.2024.3485796

Cruz-Piris, L., Marín-López, A., Álvarez-Campana, M., Sanz, M., Moreno, J. I., & Arroyo, D. (2025). Measuring the impact of post quantum cryptography in Industrial IoT scenarios. *Internet of Things, 34*, Article 101793. https://doi.org/10.1016/j.iot.2025.101793

Do, T.-B., & Tran, Q.-H. (2026). A hybrid lightweight and post-quantum communication framework for NB-IoT networks. *Microsystem Technologies, 32*, Article 37. https://doi.org/10.1007/s00542-026-06031-2

Elkhodr, M. (2025). An AI-driven framework for integrated security and privacy in Internet of Things using quantum-resistant blockchain. *Future Internet, 17*(6), Article 246. https://doi.org/10.3390/fi17060246

Halak, B., Gibson, T., Henley, M., Botea, C.-B., Heath, B., & Khan, S. (2024). Evaluation of performance, energy, and computation costs of quantum-attack resilient encryption algorithms for embedded devices. *IEEE Access, 12*, 8791-8805. https://doi.org/10.1109/ACCESS.2024.3350775

Iavich, M., Kuchukhidze, T., & Bocu, R. (2025). Fractional Verkle trees for scalable post-quantum signatures. *IEEE Access, 13*, 209921-209937. https://doi.org/10.1109/ACCESS.2025.3640288

Kerimbayeva, A., Iavich, M., Begimbayeva, Y., Gnatyuk, S., Tynymbayev, S., Temirbekova, Z., & Ussatova, O. (2025). A lightweight variant of Falcon for efficient post-quantum digital signature. *Information, 16*(7), Article 564. https://doi.org/10.3390/info16070564

Kim, C., Kwon, D., Park, Y., & Park, Y. (2026). Quantum-resistant three-party mutual authentication protocol for industrial IoT environments. *IEEE Internet of Things Journal*. Advance online publication. https://doi.org/10.1109/JIOT.2026.3677406

Kjamilji, A. (2024). Privacy-preserving zero-sum-path evaluation of decision trees in postquantum industrial IoT. *IEEE Transactions on Industrial Informatics, 20*(8), 10178-10191. https://doi.org/10.1109/TII.2024.3384523

Kundu, S., Ghosh, A., Karmakar, A., Sen, S., & Verbauwhede, I. (2025). Rudraksh: A compact and lightweight post-quantum key-encapsulation mechanism. *IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025*(2), 647-680. https://doi.org/10.46586/tches.v2025.i2.647-680

Kwon, J., Lee, S., Lee, B., Seo, H., & Cho, J. (2025). Efficient implementations of AIMer post-quantum signature scheme for low-end to high-end IoT devices. *IEEE Internet of Things Journal, 12*(22), 46817-46837. https://doi.org/10.1109/JIOT.2025.3597415

Li, Z., & Wang, D. (2022). Achieving one-round password-based authenticated key exchange over lattices. *IEEE Transactions on Services Computing, 15*(1), 308-321. https://doi.org/10.1109/TSC.2019.2939836

Mahdi, L. H., & Abdullah, A. A. (2025). A hybrid post-quantum cryptographic framework integrating Kyber-512 and ASCON for secure IoT communications. *Engineering, Technology & Applied Science Research, 15*(5), 26527-26533. https://doi.org/10.48084/etasr.12471

Marchsreiter, D. (2025). Towards quantum-safe blockchain: Exploration of PQC and public-key recovery on embedded systems. *IET Blockchain, 5*(1), Article e12094. https://doi.org/10.1049/blc2.12094

Ojetunde, B., Kurihara, T., Yano, K., Sakano, T., & Yokoyama, H. (2025). A practical implementation of post-quantum cryptography for secure wireless communication. *Network, 5*(2), Article 20. https://doi.org/10.3390/network5020020

Poomekum, P., Suriyawong, A., & Fugkeaw, S. (2025). Fine-grained and lightweight quantum-resistant access control system with efficient revocation for IoT cloud. *IEEE Open Journal of the Communications Society, 6*, 8652-8666. https://doi.org/10.1109/OJCOMS.2025.3620094

Rahmati, M., & Pagano, A. (2025). Federated learning-driven cybersecurity framework for IoT networks with privacy preserving and real-time threat detection capabilities. *Informatics, 12*(3), Article 62. https://doi.org/10.3390/informatics12030062

Señor, J., Portilla, J., & Mujica, G. (2022). Analysis of the NTRU post-quantum cryptographic scheme in constrained IoT edge devices. *IEEE Internet of Things Journal, 9*(19), 18778-18790. https://doi.org/10.1109/JIOT.2022.3162254

Shim, K.-A. (2024). On the suitability of post-quantum signature schemes for Internet of Things. *IEEE Internet of Things Journal, 11*(6), 10648-10665. https://doi.org/10.1109/JIOT.2023.3327400

Tawfik, M., Abdelhaliem, A. H., & Fathi, I. (2025). Quantum-resistant privacy-preserving IoT authentication via zero-knowledge proofs and blockchain integration. *Statistics, Optimization & Information Computing, 14*(3), 1374-1402. https://doi.org/10.19139/soic-2310-5070-2399

Wu, J., Yu, Y., Chen, Z., Yang, H., Li, C., & Liu, Z. (2025). CBPSPX: A CUDA-based batch parallel optimization of post-quantum signature SPHINCS+. *IEEE Internet of Things Journal, 12*(18), 37898-37911. https://doi.org/10.1109/JIOT.2025.3585558

Wu, W., Dong, J., Hou, Y., Liu, M., Li, L., & Dong, Z. (2026). RIGHT: GPU-optimized parallel PQC HAETAE for high-throughput cryptographic acceleration. *IEEE Transactions on Industrial Informatics, 22*(1), 532-542. https://doi.org/10.1109/TII.2025.3613305

Xu, D., Wang, X., Hao, Y., Zhang, Z., Hao, Q., Jia, H., Dong, H., & Zhang, L. (2022). Ring-ExpLWE: A high-performance and lightweight post-quantum encryption scheme for resource-constrained IoT devices. *IEEE Internet of Things Journal, 9*(23), 24122-24134. https://doi.org/10.1109/JIOT.2022.3189210

Zafar, A., & Iqbal, S. S. (2025). Integrating code-based post-quantum cryptography into SSL TLS protocols through an interoperable hybrid framework. *Discover Computing, 28,* Article 202. https://doi.org/10.1007/s10791-025-09735-7